pwc

Global Banking Risk study

Managing risk in a world of accelerating change

Foreword

Mark Batten
PwC UK
mark.batten@pwc.com

Risk functions today stand at a crossroads. The forces acting upon them are not merely episodic or one-off disruptions but also the manifestation of deeper shifts in how value is created, sustained, and contested. At PwC, we call this Value in Motion—the recognition that value and therefore the associated risk is never fixed, but constantly moving across boundaries, geographies, and systems. It is shaped by decisions, disrupted by shocks, and reframed by innovation. In this world, risk management cannot afford to be static. Its very purpose is evolving: from guardian of stability to navigator of movement, from controller of loss to enabler of resilience and growth.

This idea is more than a metaphor. It is observable in the way financial institutions operate today. Decision cycles have accelerated beyond the cadence of traditional challenge through periodic governance cycles. Technology platforms are reshaping entire functions, creating new ways of working while exposing new vulnerabilities. Leadership expectations of Risk functions have expanded: no longer limited to retrospective oversight, Risk functions are increasingly expected to generate forward-looking insight, provide clarity in ambiguity, and give business leaders the confidence to act. Value is shifting continuously—between institutions and ecosystems, between digital and human capabilities, and between regulation and innovation. Risk functions must therefore learn to track, anticipate, and influence these shifts if they are to remain relevant.

This study continues a journey we began in earlier editions in 2018 and 2022. Then, the conversation centred on efficiency, compliance, and the first signs of a pivot toward non-financial risk. By 2022, we saw the beginnings of digital transformation within Risk functions, the emergence of resilience as a board-level agenda, and an industry-wide awareness that static frameworks were falling behind the realities of modern operating environments. What has changed since then is the urgency and the scale of ambition around re-shaping operating models, data and technology strategies, and talent frameworks to increase speed, reliability and productivity.

The evidence is clear. Our dialogue with executives highlights how Risk functions are re-architecting themselves: replacing manual, human-dependent processes with cloud-enabled platforms; embedding AI to generate dynamic insight and trigger-based assurance; and rebalancing the relationship between central oversight and business-aligned enablement. Risk leaders are no longer working to preserve a steady state, but to enable organisations to operate in perpetual motion—where agility, simplicity, and intelligence matter as much as compliance and control.

Equally, the story is cultural as much as structural. Institutions are investing not only in technology and AI but also in the mindset of their people. The CRO's (Chief Risk Officer) mandate has evolved into a leadership role that emphasises collaboration, storytelling, and digital fluency. Career paths are broadening, rotations are being used to build T-shaped skillsets, and Risk executives are increasingly seen as strategic partners. These developments are not accidental; they are deliberate responses to a world where value shifts rapidly, and where resilience depends as much on an agile culture as on technical infrastructure.

This year's study takes stock of these changes and looks ahead. It is designed to serve as both a mirror and a map: a mirror that reflects the lived experience of Risk leaders navigating change, and a map that sets out pathways for capability development, regulatory engagement, and technological adoption. While no single model fits all, the underlying imperative is shared—Risk functions must be configured for motion, not just preservation.

As you read, we encourage you to reflect on your own institution's journey. Where is value moving in your business? How is your Risk function positioned to anticipate and support that movement? And what capabilities, structures, and cultures will you need to put in place so that Risk is not merely a brake but a catalyst for sustainable progress?

Executive summary

Risk function transformation is not being driven by a single catalyst, but rather by the cumulative pressures of a fast-changing geo-political and business environment: the acceleration of digital transformation, the growing complexity and interconnectedness of risk, and heightened expectations for agility, value creation, and accountability. Three forces stand out. First, growing complexity in non-financial risk areas like operational resilience, AI (Artificial Intelligence) governance, cybersecurity, and third-party dependencies. These require new capabilities, different tooling, and more dynamic ways of working. Second, executive management and Boards increasingly expect Risk to provide actionable insight—not just oversight. This means engaging earlier in the decision process, shaping strategic direction, and enabling innovation. Third, the pace of business has outstripped the cadence of traditional risk models. Risk must now match the tempo of the organisation it supports.

Architecting operating models

At the heart of this shift is the re-architecture of risk operating models, data structures and tooling platforms. Risk functions are moving beyond legacy systems and manual/overly human dependent processes to deploy modern platforms that can automate routine tasks, generate dynamic intelligence, and interact with business users in real time. These platforms are expected to be increasingly powered by artificial intelligence—particularly generative models—and configured to provide trigger-based oversight and risk tiered management rather than static, cyclical reviews. Simplicity is also being achieved through structural realignment. Risk utilities are emerging as shared services for activities such as control testing, reporting, and model development. Delegated authority and materiality thresholds are being formalised to allow business users to operate within clear risk parameters, reducing bottlenecks while maintaining oversight.

Strengthening forward-looking capabilities

Risk teams cutting across traditional functional silos are becoming more prominent in response to the changing nature and speed of business and the operating environment. The mandate of the ERM (Enterprise Risk Management) function is evolving, converging with NFR (non-financial risk) functions while uplifting top-and-emerging risk practices to anticipate required capabilities for major upcoming shifts such as quantum computing and general artificial intelligence. Significant investment is flowing into the tooling available for scenario analysis, enhancing stress testing while complementing this with modern simulation capabilities required for operational resilience as well as acknowledging the importance of qualitative expert assessments.

AI reshaping risk management

There is tangible and increasing evidence of AI fundamentally changing the shape and rhythm of risk management. Tasks that were once repetitive and manual—like reviewing remediation plans, scripting control tests, or drafting credit memos—are now being delegated to “smart tooling” or intelligent agents. These tools augment human decision-making, streamline execution, and unlock new possibilities for pattern detection and predictive analytics. Productivity remains the dominant use case. Firms are deploying GenAI (Generative Artificial Intelligence) to reduce friction in document-heavy processes, increase the speed of insights, and improve consistency in decision-making. Risk functions are seeing early wins in credit, fraud, compliance, and non-financial risk monitoring. Use cases include real-time AML (Anti Money Laundering) flag resolution, policy simplification through natural language processing, and agent-driven assurance models that monitor operations autonomously.

NFR 2.0 – Rethinking NFR with a spotlight on Resilience

Rethinking non-financial risk and resilience has become a defining theme in the 2025 risk agenda. This shift is being driven by geopolitical uncertainty, climate-related events, supply chain disruptions, and an increasing reliance on a concentrated set of technology providers. The resilience agenda also extends beyond the firm's perimeter. Concentration risks related to cloud and AI vendors are prompting fresh dialogue on strategic dependence, vendor assurance, and regional technology sovereignty. Some firms are revisiting third-party governance models, while others are collaborating with regulators and industry groups to stress test shared vulnerabilities and contingency plans. Critically, resilience is being embedded into broader transformation initiatives. Digital twins, scenario analysis platforms rooted in process intelligence, and cross-functional resilience squads are helping firms design for complexity and unpredictability - not merely recover from disruption.

Sustainability coming under pressure

While most firms remain committed to sustainability targets, geopolitical and regulatory divergence are formidable challenges that are increasingly difficult to navigate. The transition of society provides significant opportunities for financial services to partner with governments and industry; yet more remains to be done on building fit-for-purpose analytical capabilities. Taking stock of the experience of the past five years, there is a call for a step back to establish common foundations via common taxonomies and data models. There is also a need to strengthen this with common protocols for data capture and exchange across society. Finally significant differences in interpretations and practices highlight the opportunity to review the perimeter of ESG. This includes, for example, sharpening the focus on climate and environmental risk while ensuring that lessons learnt are reflected in the political and regulatory approach for nature risk.

Resetting of the regulatory relationship

A cornerstone of the evolving risk landscape is the ambition to adjust the relationship between financial institutions and regulators. The current model—prescriptive, static, and often fragmented—is struggling to keep pace with innovation in AI, ESG (Environmental, Social, Governance), operational resilience, and third-party dependency. Institutions are advocating for co-development of standards, greater clarity in supervisory expectations, and more iterative engagement. This includes enhancing practices such as formal feedback cycles and joint sandboxes while emphasising international alignment on critical issues like digital identity, data provenance, and AI liability.

Transformation of Leadership and talent

Finally, within firms, the leadership model for Risk is also evolving. Succession planning and talent development are gaining focus. Institutions are moving away from narrow, siloed career paths toward broader, rotational journeys that build holistic, T-shaped profiles. Leadership programmes now emphasise not just technical mastery, but collaboration, storytelling, and digital fluency.

Contents

01 Risk branding and operating model - Emphasis on strategic and commercial enablement while re-balancing from financial to non-financial risks

The brand and mandate of Risk functions is undergoing a significant change. In prior studies (2018 and 2022), the spotlight was largely on efficiency, compliance, and non-financial risk increasingly rising up the agenda. Since then, the pace and scope of change have accelerated. Risk is no longer viewed solely as a guardian of stability; it is being reshaped into a function that enables strategy, innovation, and resilience.

Compared to previous studies, we observe a clear increase in emphasis across three areas that define the trajectory of Risk transformation:

1. Risk brand and mandate — consensus across executives on the need for Risk to deliver greater strategic and commercial value, extending beyond oversight into helping shape business choices and enabling growth.
2. Operating model — as institutions rethink how Risk is organised, integrated, and scaled, with new structures, utilities, and cross-functional alignment designed to improve agility and intelligence.
3. Culture and mindset — increasingly recognised as critical enablers of transformation, embedding the new mandate through behaviours, leadership tone, and interaction models.

The sections that follow explore each of these three themes in turn.

Risk brand and mandate

Risk functions are increasingly seen as a dynamic enabler of sustainable growth, and an active part of organisational transformation with a focus on efficiency, innovation and a great customer experience. While this, by no means, replaces the existing mandate of oversight and challenge, Risk functions are clearly expected to do more.

Institutions describe that this is being translated into practice by giving Risk functions a more prominent role in various activities:

Table 1: How institutions are giving Risk a more prominent role

Theme	Description
Shaping strategy and planning	Being more active in the risk/reward discussion (e.g., corporate planning) while providing insights and analytics to enable the evaluation of different business and operating model choices. This includes greater emphasis on risk appetite in decisions such as sourcing and technology
Empower 1st line through clear boundaries and minimal red-tape	Emphasising delegated authority and materiality-based decision-making. For example: • Risk's role in credit continues to shift toward portfolio management, with more automation and delegated authority speeding up decisioning • Embedding a focus on materiality and evolving the interaction model for new product approvals and third-party onboarding • Emphasising risk acceptance in issues management is significantly reducing effort while not compromising effectiveness
Tooling and data	Building tooling and analytics platforms that add business value and contribute to end-to-end efficiency (e.g. customisable control environment dashboards). There is a strong emphasis on pan-organisational efforts as part of data and infrastructure programs, which are critical to competitiveness

These areas have always been important, yet there is a notable shift in emphasis across the industry. This is strongly reflected in organisational choices and a focus on culture and mindset as key enablers to get this right.

Risk operating model

Over the past three years, institutions have made notable adjustments to the way Risk is structured and organised. While the industry still largely maintains separate second line functions for Risk and Compliance, reporting lines and mandates are evolving, and new operating constructs are being tested.

A small number of firms have trialled integrated NFR and Compliance functions, though most continue to prefer alignment of taxonomies, processes, and tooling rather than full structural merger. Beyond structural shifts, there is growing attention on how Risk engages with the business, how analytics capabilities are scaled, and how efficiency is achieved through centralisation. These developments highlight a wider movement toward more agile, forward-looking, and technology-enabled models.

Table 2: Operating model themes

Theme	Summary
Risk and Compliance structures	Most institutions maintain separate second line functions for Risk and Compliance. In ~50% of cases, the Chief Compliance Officer reports into the CRO. A small number of institutions integrate NFR and Compliance under a separate board-level executive, but most prefer alignment of taxonomies, processes, and tooling. Institutions are further strengthening teams which cut across traditional risk stripes like Credit/Market/Operational, putting equal emphasis on forward-looking risk landscape and stronger roles for ERM and NFR teams
Embedding Risk through agile and business-aligned ways of working	There is a growing focus on realigning Risk functions to business lines. Business-aligned CROs / teams are established as single points of contact, providing holistic support to business, reducing the number of touch points and speeding up processes. Perspectives on this construct highlight that it works well for specific processes like product approvals and third-party onboarding. However, there are limitations in more complex questions where deep expertise is required throughout, e.g. in the deployment of novel tooling such as embedding "smart" agents in assurance processes. There is no clear answer to this topic across industry, with evolution of organisational models expected in the coming years
Enhancing forward-looking and holistic capabilities	ERM and NFR are highlighted as investment areas to enhance forward-looking and holistic analytics capabilities. Since our last study, we see the following key changes: • ERM: A growing mandate component is a forward-looking think tank, providing enhanced horizon scanning, strategic and longer-term insights shaping strategy and analysing required capabilities to manage the risks of emerging disruptors including AI and Quantum Computing • Convergence of ERM and NFR: ERM and NFR have similar facets in focusing on driving thematic and forward-looking insights and analytics into the organisation. There is increasing engagement between ERM and NFR in building out capabilities and management information, with some organisations having established an integrated reporting structure into a single individual There is further an emergence of centres of excellence in complex areas such as digital risks and AI. Examples include fusion centres for informational, cybersecurity, technology risks / resilience (cross-functional structures integrating different teams, data and analytics capabilities) as well as AI governance, which joins up MRM (Model Risk Management) with functions including Data, Technology, Legal and Compliance
Centralisation to drive standardisation, digitisation and economies of scale	Transformation programs are emphasising centralisation of high-effort activities, with a growing focus on using this for longer-term operating model transformation. Key focus areas highlighted across the industry include assurance processes, reporting production and modelling / analytics This includes centralisation across functions and lines of defence, with emerging dialogue on establishing utilities providing risk and control assurance services across different lines of defence. There are individual banks that have established assurance utility mandates across financial and non-financial risks, yet this has yet to translate into an industry-wide trend. Centralisation strategies are closely linked to standardisation, digitisation and sourcing initiatives The outlook for centralised activities is to provide a platform for targeted GenAI deployment, driving at-scale automation of processing and production activities that retain a significant manual component
Industry utilities – towards centralised standards and services	Extending the thinking on centralisation, there are areas where industry utilities providing services to a range of institutions could be beneficial. This includes a call for bodies developing common protocols and pooling data in the domains of ESG and NFR, as well as organisations providing centralised services such as specialist valuations or assurance activities
Beyond the perimeter of the organisation – systemic risk of technology companies	Institutions have become increasingly dependent on a small set of critical third-party providers—especially in cloud and AI. This makes these companies a key component of the organisation Risk perimeter, raising systemic resilience concerns Some banks highlighted that in the medium term, there could be a growing drive for reassessment of regional technology sovereignty and potentially diversifying current strategic concentrations in a handful of critical providers. Nevertheless, there is consensus on the need to strengthen integration with third-party assurance mechanisms to mitigate risks

Culture and mindset

Compared to earlier studies, culture and mindset are now seen as decisive enablers of change. Organisations are adopting deliberate programmes to reshape culture, behaviours, and interaction models, based on broadly consistent objectives across the industry.

Table 3: Industry focus areas in changing culture, interaction models and behaviours

Theme	Summary
Commercial enablement and collaboration	Risk is being repositioned as an enabler of commercial success, faster time-to-market, and stronger customer experience. Institutions emphasise a "yes, but" mindset—setting risk-informed guardrails rather than defaulting to "no." The second line's role is shifting away from policing toward partnership, supporting innovation while ensuring resilience. In some organisations, we have seen this translate into more agile 3LOD models regarding interaction across first and second lines of defence
Agility through simplification and risk based decision making	Interaction models are being redesigned to focus on materiality and delegated authority. This includes empowering business teams to act within clear boundaries while Risk monitors at portfolio level, introducing single points of contact for approvals and onboarding, and breaking sequential engagement cycles by moving toward early and iterative Risk involvement
Leadership and behaviours	Culture change is being driven from the top, with executives role-modelling behaviours and mid-level leaders empowered to bridge legacy processes and innovation delivery. Actions include breaking down senior-level silos tied to budget and accountability, adjusting metrics, using rotations to build T-shaped profiles, and actively managing target behaviours
Ways of working and skills	Organisations are building collaborative structures based on shared data, tooling, and analytics to reduce friction and enable continuous improvement. Skills priorities include entrepreneurship, problem-solving, and holistic thinking (e.g., credit experts also understanding data, fraud, and process design). Continuous learning and adaptability are embedded into culture to prepare for an AI-driven future

Organisations that have emphasised culture and mindset pointed to tangible benefits, including lower cost income ratios, faster speed to market and faster change / innovation cycles. Examples provided include:

- Solving problems in cross-functional squads, such as bringing down fraud or taking 2 minutes to issue a new credit card
- Reducing operational expenditure by embedding a rigorous efficiency mindset in culture, including much lower spend on external services
- Embracing a continuous improvement and innovation mindset, with teams driving digitisation and automation within their remit – a trend expected to be amplified by GenAI

02 Non-Financial Risk Management 2.0 - An emerging blueprint for a digital and connected institution

As non-financial risks rise in prominence, they are bringing new complexity, urgency, and interconnectedness that legacy frameworks and cultures were not designed to handle. Institutions increasingly recognise the need to pivot to more forward-looking practices: embedding accountability at every level, enabling resilience in an unpredictable world, and building digital capabilities that reflect how organisations operate today.

Yet progress is uneven. Non-financial risk remains the area with the widest maturity spectrum across the industry. Some institutions are only beginning to address foundational issues such as accountability, taxonomies, and data quality, while others are already experimenting with digital twins, AI assistants, and integrated resilience platforms. What unites them is a recognition that non-financial risk can no longer be managed as an afterthought: it must be embedded in business design, supported by modern architectures, and enabled by new ways of working.

Compared to our 2018 and 2022 studies, we now see stronger emphasis in four areas:

- A continuing shift in focus from financial to non-financial risks, creating capacity and attention for modernising capabilities.

- A drive to fix the foundations, through clearer taxonomies, data models, and accountability structures.
- The emergence of next-generation architectures, where non-financial risk and resilience are managed through integrated, digital views of process and control landscape i.e. digital twins.
- Early experimentation with AI augmentation, using automation, assistants, and pattern detection to transform how risk is experienced and actioned.

This transformation is not theoretical—it is already underway. Firms are moving from fragmented processes to integrated platforms, from static reports to dynamic intelligence, and from reactive control to forward-looking engagement. At the centre of this evolution lies a new kind of risk architecture—one that connects people, processes, data, and AI to deliver value and insight, not just assurance

The sections that follow illustrate how this blueprint is beginning to take shape across the industry.

Pivoting from financial to non-financial risks requires a repositioning of Risk across core businesses and processes

There is broad industry consensus that financial risks are under control, with robust skills and capabilities. Most organisations emphasised the shift of CRO focus towards non-financial risks, with the need to revisit organisational structures while building capabilities embedded through cultural transformation.

This pivot has been underway for several years, with varying degrees of progress. However, the repositioning of Risk's role in financial risks in an effort to reallocate capacity towards building NFR capabilities is increasingly evident. Key challenges and measures that industry has taken in response include the following:

Table 4: Characteristics, challenges, and transformation levers across non-financial risks

	Key challenges	Measures taken
First line accountability	A persistent lack of accountability and capability in the first line, with the assumption that this is "Risk's role". While on aggregate there has been progress since our last study, this remains a significant obstacle for many institutions	• Making first line executives accountable for the risk and control profile at Risk committees and in regulatory / audit forums • Enhancements to core tooling provided by the second line, designing it to be intuitive and "customer-friendly" • Simplification of interaction models and materiality-driven workflows (e.g. for new products / third party onboarding)
Specialist expertise in the second line	Need to uplift second line capabilities in resilience, cybersecurity, and AI, amid a volatile geopolitical landscape Too much capacity remains bound in low value "backward" looking activities, with a need to unlock reinvestment into specialist skillsets	• Establish centres of excellence / cross-risk structures to better govern and control complex thematic and digital risks • Collaborative structures to build out core tooling and analytics between business, infrastructure and non-financial risk teams
Building digital and scalable foundations	Inconsistent taxonomies and practices embedded in tooling leading to fragmented and manual processes	• Investment in consistent taxonomies and data models; embedding this in next-generation architectures • Building integrated and automated management information, with focus on actionable indicators and read-across to broader business and financial reports

A need to fix the foundations by focusing on mindset, taxonomies and data

While there is growing recognition of the importance of non-financial risk, many of the most persistent challenges arise from deep-rooted cultural and structural issues.

Figure 1: Biggest challenges in effectively managing non-financial risks[1]

	Average ranking	Number 1 choice
Fragmented and manual intensive processes	2.7	5
Poorly designed GRC systems	3.3	1
Lack of first line engagement / accountability	3.5	4
Burden of regulatory remediation leaves no time for transformation	3.5	6
Lack of access to operational data	3.6	1
Lack in innovative culture / fresh thinking	4.3	1

Regulatory remediation for example remains a key challenge for many organisations, consuming extensive resources. It also drives a "backward-looking" staff mindset and a perception that non-financial risk is a burden rather than a critical capability. Similarly, accountability remains a challenge across all maturity levels. Numerous institutions explained that first-line functions often still see non-financial risk as a job of the Risk function, rather than embracing it as their core accountability.

A step-change is now underway. Institutions are redesigning taxonomies and data models, shifting toward process- and product-based views of the organisation. This anchors NFR in business reality, enabling joined-up views of risk, resilience, and operations.

Table 5: Foundations for future-proof NFR capabilities

Focus Area	Emerging Practices
Taxonomies	Taxonomies are being redesigned around products and processes to provide an end-to-end view of operations. Mapping assets (technology, premises, third parties) to processes creates a basis for integrating NFR and resilience
Data quality	Data remains fragmented, inaccessible, and low quality. Risk teams in leading firms are collaborating with Chief Data Offices to shape data models, define standards, and cleanse datasets for use in advanced analytics
Legacy architecture challenges	Despite progress, legacy systems still present formidable obstacles. Many firms expect multi-year journeys to modernise architectures and unlock full use of data
Industry convergence	Common standards are beginning to emerge, with several firms pointing to ORX-led reference models that help firms converge on shared taxonomies and data approaches (e.g. risk, process, product and control taxonomies) for NFR and resilience

1 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

The criticality of taxonomies and data cannot be understated, as this provides the basis for the configuration of systems enabling digital, consistent and scalable management of non-financial risks. Many participants believe that this further presents an opportunity for the discipline to mature overall, pointing to ongoing efforts to develop common reference models that could help firms converge around shared standards for NFR and resilience.

Next generation GRC systems will be centred around a digital twin of the organisation

Leading institutions are moving beyond incremental improvements and are designing next-generation architectures for NFR and operational resilience. Their ambition is to establish a digital twin of the organisation which sets out a comprehensive digitised version of how processes and controls actually operate.

This approach anchors risk models in business reality: structuring taxonomies around value streams, products, and services. These frameworks are not static lists of risks, but functional maps of how organisations operate, how services are delivered, and where vulnerabilities lie. By aligning taxonomies with operational processes, firms are creating a common language that bridges silos, connects risk and resilience, and integrates across the three lines of defence.

The benefits are tangible:

- Risks, controls, incidents, and resilience scenarios can be coherently mapped across the enterprise.
- GRC platforms shift from data collection to insight generation.
- Standardised taxonomies unlock opportunities for cross-industry collaboration.

Table 6: Features of a next-generation NFR and resilience architecture

Element	Description
Process/product taxonomy	A consistent taxonomy is deployed across the organisation and used by all lines of defence, giving an end-to-end view of value streams at process-step level. Assets (technology, premises, third parties) are mapped to these processes
Automated data ingestion	Automated data feeds integrate existing and new datasets through defined protocols. Quality assurance and transformation practices are applied before data can be used
Cloud tooling	Cloud capabilities extend beyond computation to include data quality management, knowledge graphing and AI integration, providing a foundation for sophisticated analytics
GRC tooling	Core GRC processes are anchored in taxonomies and data models, ensuring alignment across the lines of defence. Intelligent agents are embedded, capable of executing tasks directed by risk managers
Management information and steering	Customisable dashboards and trigger-based assurance provide real-time insights and AI-enabled analytics and response capabilities

Augmentation of non-financial risk and resilience managers – pattern analytics, agents and digital risk assistants

Historically, non-financial risk teams have been perceived as reactive – focused on post-incident analysis, regulatory compliance, and retrospective reporting. This posture, though born from necessity, limited the perceived strategic value of risk professionals and created a sense of fatigue across the function. But as technology matures, firms are starting to unlock a different model: one where AI augments judgement, automation removes friction, and data enables forward-looking insight.

Firms are now actively experimenting with ways to digitise risk management, not just to gain efficiency, but to fundamentally evolve how risk is owned, experienced, and actioned. From deploying AI assistants to reshaping GRC processes entirely, this is not just an enhancement—it's a redefinition of the Risk function's purpose and potential. The grid below summarises how firms are making this shift a reality.

Table 7: How Firms Are Digitally Augmenting the Risk Function

Element	Description
Freeing up capacity through automation	Using AI to review remediation plans, monitor control effectiveness, script automated tests
AI-powered risk assistants	Deploying chatbots and virtual agents that interpret policy, guide risk users, and interact with GRC systems
Task prioritisation through AI planners	Smart tools that help frontline staff identify and prioritise high-risk actions on a daily/weekly basis
Predictive analytics and pattern detection	Correlating operational and risk data to flag early warning signals (e.g., incident clusters, access anomalies)
Reimagining legacy processes (e.g. RCSA)	Exploring whether AI agents could replace annual reviews with regular, interactive engagement based on real-time data
Building momentum through modular deployment	Starting small with targeted AI use cases to demonstrate value and overcome resistance
Executive sponsorship and mindset shift	Securing leadership support for treating risk as a strategic lever, not just a control function

The AI deployments described above are at early stages, but individual firms are running agents and have had initial versions of digital risk assistants up and running for several years. This is not just augmenting Risk capabilities. There are firms that have deployed agents in digital first line risk and control teams, and one firm is redesigning its end-to-end RCSA (Risk and Control Self Assessment) process to embed regular intra-month interaction using AI agents. The future is here and the next five years will see a fundamental change to the way in which non-financial risks are being managed.

03 The AI Transition - From tactical innovation to organisational redesign

As generative AI moves from early experimentation to enterprise adoption, financial institutions are facing a structural transition in how work gets done, how risk is managed, and how control is maintained. This is not simply a wave of new technology—it is reshaping workforce models, accountability structures, and organisational design. AI is no longer confined to analytics teams or innovation hubs; it is being woven into the daily routines of staff, and increasingly into the decision-making architecture of the firm. Institutions must therefore rethink the operating model for Risk—balancing experimentation with governance, decentralised adoption with central control, and productivity gains with new and amplified exposures.

Compared to our 2022 study, four themes stand out:

- A structural shift in workforce and adoption strategies, as firms move beyond experimentation to new models of human–AI collaboration.
- The rise of productivity-focused use cases, especially in credit and non-financial risk, where AI is streamlining effort-heavy processes.
- An urgent need for new governance and control mechanisms, as existing model risk framework struggle to address GenAI's opacity, unpredictability, and scale of adoption; and what will fall in the scope of formal validation practices.
- An expanding risk perimeter, with AI amplifying systemic risks in trust, authenticity, security and third-party dependencies.

The following sections examine each of these dimensions in turn.

A structural shift – transformative vision yet different adoption strategies

GenAI deployment at scale is still in its early stages, yet it is already prompting a re-examination of foundational assumptions about the economy, work, and control. Advances in AI capabilities are ushering in a vision of a hybrid workforce—one in which a smaller number of highly skilled professionals work alongside increasingly capable AI agents. This evolution is not just about automation of repetitive tasks; it represents a deeper shift in how institutions allocate judgement, oversight, and value creation. In this new model, humans transition from task executors to supervisors and orchestrators of AI-driven activity.

This transformation brings immense opportunity—but also disruption. The social implications are significant, ranging from employment stability to the potential for transitional fractures in the workforce. Most institutions do not see this shift as optional. GenAI is becoming a competitive imperative, with most firms now moving beyond caution and into active experimentation. There is a growing realisation that embracing AI is central not only to productivity, but to talent strategy, innovation, and long-term viability.

However, adoption strategies are not uniform, representing a continuum between prudence and large-scale adoption, with most institutions in the first two categories:

Table 8: GenAI adoption strategies across industry

Strategy	What Firms Are Doing	Implications
Centralised	Strong governance bodies approve/oversee enterprise-level use cases; dedicated AI teams develop solutions within Technology or Analytics	Enables control and consistency; may slow experimentation
Federated	Small AI teams embedded within functions (e.g., Risk) actively experiment with GenAI; business-aligned innovation	Enables local ownership; risks fragmentation if not coordinated
Democratised	Broad access to GenAI tools; mid-level leaders monitor usage while fostering creativity and uptake	Encourages adoption at scale; requires cultural guardrails and oversight

Banks highlight a diverse set of key AI challenges with broad consensus on infrastructure investments, bespoke data and skillsets as top issues. Infrastructure is closely linked to data availability and readiness as well as the maturity of process digitisation in deploying AI for productivity use cases. On the skills side, there is not just fierce competition within financial services, but also versus other industries; pointing to the need of a broader skills strategy around AI. Regulation was not highlighted as a key challenge on average. However, the first major AI disruption / failure, which may occur outside the financial services industry, is commonly expected to lead to significant political and regulatory fall-out. Whatever the choice of adoption strategy, regulation should be a key consideration over the coming years.

Figure 2: Key impediments faced in the adoption of AI[2]

	Average ranking	Number 1 choice
Infrastructure Investment	2.5	7
Bespoke Training Data	2.6	5
Scarce or Expensive Skillsets	2.8	4
Tangible Return on Investment	3.2	3
Unclear Regulation / Regulatory Risks	3.7	3

From productivity to possibility – AI use cases are gaining traction in Risk

Many institutions have actively deployed GenAI in production, with most use cases concentrated in parts of the organisation outside Risk. The primary focus remains productivity uplift, with firms generally limiting GenAI deployment in direct customer contact for the time being. This observation holds true for Risk functions as well: while the number of direct Risk use cases appears low, Risk is deeply involved in shaping deployments that enable productivity and efficiency across the organisation. Successful firms tend to apply two criteria when selecting use cases: (1) significant effort is currently required, and (2) the task has a repetitive or standardised dimension.

Figure 3: Number of GenAI models in production across the organisation[3]

	Number of GenAI models in production				
	0	**1-5**	**5-10**	**10-20**	**>20**
In Risk	9	6	2	0	0
In other organisational areas	2	6	4	3	2

2 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

3 Table shows the count of responses by participants indicating a specific range of GenAI models in production

Figure 4: Success and opportunities in deploying GenAI[4]

	Success	Opportunities
ERM	1	2
Credit	9	7
NFR	4	5
Compliance / Fincrime	17	7
Modelling and analytics	1	2
General productivity and decisioning	10	21

Early adoption has been prominent in credit processes, where sentiment analysis, early warning, and document generation (e.g., credit memos) are gaining traction. Firms are also experimenting with quality assurance and information filtering. In non-financial risk, AI has proven valuable in high-throughput areas such as fraud detection and AML/KYC (Know Your Customer). One institution, for example, has reduced AML hit processing time from an hour to 20 seconds. A further area of focus is simplifying engagement with frameworks and systems—whether through natural language policy queries or redesigned GRC interfaces. Other common areas include traditionally hard challenges such as a central register of obligations, policy simplification and engagement.

Some institutions are pushing further. One has operated a digital risk assistant for several years, while others are piloting agents that digitise first-line assurance activities. This is expected to be among the most transformative areas in the years ahead, with more sophisticated AI applications driving a transition to a hybrid workforce. Risk managers will increasingly oversee digital agents rather than complete every task themselves. There is even exploratory work on using GenAI's so-called "hallucinations" to imagine novel threat scenarios, for example in fraud or cyberattack modelling.

Table 9: Approaches and focus areas in deploying AI tooling

Theme	What Firms Are Doing
Productivity-Led AI Use	Automating effort-intensive, repetitive tasks
Credit and Control Processes	Deploying GenAI in underwriting, memo generation, control reporting
Policy Simplification and Engagement	Using NLP (Natural Language Processing) tools to interpret and summarise rules. Using natural language querying to engage with policies
Early Warning Systems	Integrating sentiment and pattern analysis into risk tooling
Agentic AI Pilots	Testing semi-autonomous agents in risk execution
Innovative Threat Modelling	Prompting LLMs (Large Language Models) to invent future threat scenarios (e.g. fraud, control failures)
Centralisation Synergy	Aligning AI deployment with restructuring initiatives

4 Table based on the top 3 GenAI use cases indicated by study participants

How to govern and control AI – towards multidisciplinary oversight

As GenAI diffuses across the enterprise, financial institutions have increasingly realised that traditional governance models - especially those inherited from model risk management - are no longer sufficient. While MRM frameworks provide a conceptual base (e.g., tiering models by materiality, tracking performance), they fall short when dealing with AI models that are non-deterministic, opaque, or embedded in third-party tools. GenAI introduces interpretability challenges, behavioural unpredictability, and legal/ethical ambiguity at a level most existing control frameworks were not designed to handle.

A further challenge lies in controlling democratised AI use, where staff are actively encouraged to use the technology in everyday tasks. While some exclusions and after-the-fact checking can be applied, "live" control capabilities do not currently exist.

Most organisations have a dedicated AI policy in place but recognise this requires a broader approach than traditional structures. Centres of excellence are being established to bring together disciplines such as MRM, Legal, Compliance, Technology and Data, and Privacy. These bodies govern central use cases while coordinating control design for decentralised usage—including LLM access rolled out to large teams. This governance extends beyond risk management into broader ethical considerations of where AI should and should not be used.

Finally, cultural considerations are becoming critical. Several participants expressed concern about staff overreliance on GenAI outputs at the expense of judgement and critical thinking. This is expected to be a key leadership focus in establishing the right mindset for the GenAI era.

Table 10: Establishing governance and control practices for AI

Theme	What Firms Are Doing	Governance Implications
Beyond traditional MRM	Recognising gaps in existing model control frameworks	Prompting evolution of new AI-specific assurance layers
Central use case governance	Establishing governance mechanisms for selection, development, and implementation of enterprise-level use cases; clarifying when model validation is required	Supports oversight of high-impact deployments; defines level of assurance needed
Multidisciplinary governance	Creating joint AI oversight forums across MRM, Legal, Compliance, Technology and Data, and Privacy	Provides a coordinated view of complex risks
Democratised AI controls	Monitoring federated and democratic use; applying behavioural nudges, log reviews, and cultural guidance	Balances creativity and productivity with oversight; acknowledges limits of technical guardrails
Third-party AI oversight	Assessing AI embedded in vendor solutions and mapping dependencies	Addresses risks outside the firm's direct control; improves transparency on hidden exposures
Staff over-reliance concern	Training staff to maintain critical thinking and challenge	Prevents cognitive offloading and blind reliance on AI outputs
Validation innovation	Testing proxies, challenge models, and audit mechanisms	Progress toward interpretability and traceability
Human-in-the-loop assurance	Mandating checkpoints before final actions	Safeguards decision quality while governance matures

A broader risk perimeter – From internal fragilities to societal exposure

As AI adoption accelerates, the boundaries of organisational risk are expanding. What began as a conversation about internal model performance has quickly become a dialogue about systemic exposure. The inability to detect and mitigate erroneous outputs from AI models remains a core concern—particularly in areas like credit decisioning or customer interaction where errors can be high impact and hard to trace.

Figure 5: Key risks from GenAI inside and outside the organisation[5]

	Inside organisation	
	Average ranking	Number 1 choice
Inability to identify / mitigate erroneous analysis and decisions	2.6	10
Data Privacy / Leakage	3.3	4
Fake Information	3.5	3
Cybersecurity	3.7	0
Third Party Risk	3.9	2
Financial Crime	4.8	1
Individuals (staff, customers, society) becoming more reliant on AI	5.5	0

	Outside organisation	
	Average ranking	Number 1 choice
Cybersecurity	2.4	6
Fake Information	2.7	4
Financial Crime	3.4	2
Data Privacy / Leakage	4.0	1
Inability to identify / mitigate erroneous analysis and decisions	4.1	4
Third Party Risk	4.9	1
Individuals (staff, customers, society) becoming more reliant on AI	5.9	0

Third-party integration is a growing risk. Banks increasingly rely on external vendors whose platforms incorporate AI by default, creating hidden dependencies, limited visibility, and potential spillover effects—especially when those vendors operate outside the regulatory perimeter.

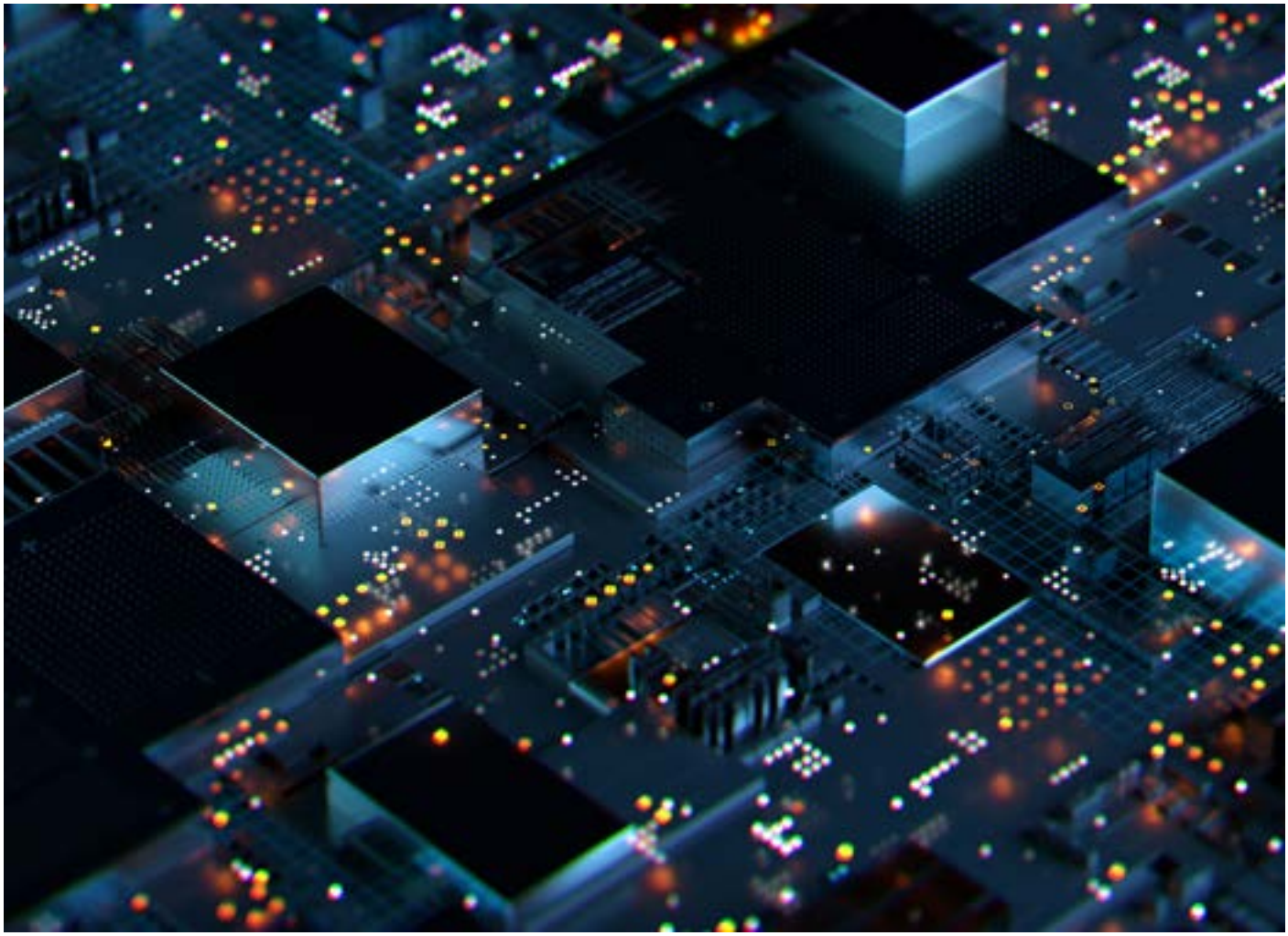
Externally, AI is also reshaping the landscape of trust and authenticity. More convincing impersonation, synthetic content, and misinformation are pulling financial institutions into a broader societal risk arena. Verification of digital identity is becoming a critical challenge: while some firms are embedding verification tools into customer apps, there is consensus that digital identity cannot be solved by institutions alone and requires regulatory and political dialogue and solutions.

At the macro level, leaders are worried about AI's potential to erode collective trust. Weaponised misinformation and synthetic media are seen as amplifiers of societal instability. While this extends beyond the traditional remit of banks, many believe the sector must engage more actively in shaping safeguards for a digital society.

5 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

Table 11: Responding to the amplification of risks via GenAI

Theme	What Firms Are Doing	Governance Implications
Error Detection Gaps	Prioritising model validation and human oversight	Concern over undetected or systemic errors
Third-Party AI Risk	Identifying embedded AI in vendor solutions, mapping dependencies	Low visibility into tools outside firm perimeter
Customer Verification	Building in-app validation tools for outreach authenticity	Attempting to close trust gap in digital interactions
Responsibility and Liability	Calling for shared accountability in fraud outcomes	Push to rebalance risk away from banks alone
AI-Enabled Criminality	Monitoring GenAI use in fraud, impersonation, deception	Increased scale and sophistication of threats
Erosion of Trust	Recognising systemic impacts of fake content and misinformation	AI seen as amplifier of societal instability
Regulatory Advocacy	Urging collective standards for identity, fraud and misinformation	A move toward societal-level safeguards and frameworks



04 Navigating Social, Political and Technological Uncertainty - From social media to tariffs and quantum computing

The past decade has seen relentless acceleration of change, driven by deep structural shifts across geopolitical, environmental, and technological dimensions. A fracturing of global alliances and rising protectionism have begun to challenge long-held assumptions about international cooperation, trade flows, and strategic partnerships. These shifts carry far-reaching implications—undermining global climate coordination, reshaping food systems and supply chains, and straining social cohesion.

In this context, there is growing consensus that today's risk structures, methodologies, and tooling are no longer fit for purpose. Institutions recognise the need to modernise—from static frameworks to adaptive systems capable of navigating dynamic, systemic risk. Four themes are emerging in how firms are responding:

- Redefining the ERM mandate, so that Risk can move from reactive to proactive and anticipate disruptive trends.

- Broadening the forward-looking toolkit, with stress testing and scenario analysis becoming faster, more flexible, and better suited to today's uncertainty.
- Investing in early warning systems, leveraging new data sources while addressing risks from corrupted or falsified information.
- Confronting strategic dependencies, especially growing reliance on technology providers, which raises questions of resilience and sovereignty.

The following subsections explore each of these themes in turn.

From reactive to proactive – Evolving the Enterprise Risk Management function

Risk remains too reactive and backward-looking, with a need to enhance forward-looking capabilities. While processes such as horizon scanning and top-and-emerging risk monitoring are in place, their use of insights has fallen short of anticipating the capabilities required when major trends or disruptive changes materialise. In today's environment of accelerating change—with looming implications of quantum computing, the expanding role of AI, and a fragmenting world order—this shortfall is increasingly recognised as a strategic gap.

In response, an emerging trend is the expansion of the Enterprise Risk Management function's mandate into a "think tank" role, tasked with working through the implications of major trends and risks. The focus is on establishing a framework to assess complex disruptors, identify the critical questions, and determine what capabilities may be required in response. ERM teams are connecting experts within and beyond the organisation, with careful curation of themes given the significant demand on specialist time. The range of complex themes raised in our discussions underscores the urgency of elevating current forward-looking capabilities to the next level.

Table 12: Industry perspectives on core industry disruptors over the next decade

Theme	What Firms Are Doing	Governance Implications
Quantum Computing	Prototypes are progressing, increasing the likelihood of scalable quantum systems within the next decade	– Potential for current encryption to be broken, compromising secure data exchange – Sensitive information may be exposed retroactively – Requires early design of post-quantum frameworks
Artificial Intelligence	Over the medium term, AI is expanding in scope and application across society, with potential for significant upheaval to labour markets and political stability The spectre of general artificial intelligence is becoming real and may fundamentally alter the way the global society functions	– Disruption to employment and operating models – Need for explainability and control – Emergence of general artificial intelligence
Synthetic Media / Fake Info	Manipulated video, audio, and text is becoming indistinguishable from real content	– Escalating fraud and cybercrime risks – Erosion of customer trust – Systemic risk from political or social destabilisation
Digital Assets & Tokenisation	Growing regulatory support and political support in the US is accelerating adoption and integration of digital assets into the financial system	– New asset classes with novel risk profiles – Infrastructure and custody risks – Uncertain compliance and valuation frameworks
Geopolitical Shifts	Global power dynamics are shifting, undermining multilateral institutions and fragmenting policy responses	– Volatile trade conditions and regulatory fragmentation – Amplifier of other risks, including energy, cyber, and inflation shocks

Stress-testing and scenario analysis: Evolving the forward-looking toolkit while investing in faster and more dynamic production capabilities

The complexity and pace of today's environment demand a fundamental uplift in how organisations use stress testing and scenario analysis. Traditional approaches—designed for relatively stable conditions—are too slow, too rigid, and too focused on regulatory requirements, rather than decision-useful insights.

Since our 2022 study, industry reflection on the **limitations of stress testing** has deepened. While stress testing established itself as a powerful tool after the global financial crisis, it works best within a specific perimeter. For more complex topics such as operational resilience or climate change, other approaches—like **qualitative scenario analysis** and **system simulations**—are increasingly being adopted to capture second- and third-order effects that stress testing struggles to address.

At the same time, firms are modernising core stress testing processes. End-to-end production remains anchored in Finance for most, with cycle times of four to six weeks, which is no longer compatible with today's speed of change. Institutions are therefore investing in faster production cycles, modular architecture, and analytics platforms, enabling more frequent, flexible, and decision-relevant insights.

Table 13: Expanded Toolkit for Scenario and Resilience analysis

Capability	Description	Use Cases
Enhanced Stress Testing	More frequent and flexible scenario execution, moving beyond slow, Finance-anchored processes that often take 4–6 weeks	– Self-service scenario access for business units – Faster response to geopolitical shocks – Monitoring of critical thresholds
Process / Ecosystem Simulation	Using system dynamics to simulate interconnected processes and ecosystems; closely linked to process digitisation in resilience	– Testing resilience of payment systems under IT failures or cyberattacks – Simulating production and operational processes. – Evaluating structural business model changes
Qualitative Scenario Analysis	War-gaming, storytelling, and structured expert assessments to explore unquantifiable risks	– Operational implications of trade conflicts (e.g., tariff war) – Geopolitical conflict spillover (e.g. Europe). – Anticipating second/third-order effects
Hybrid Tooling & Integration	Combining scenario outputs with dashboards and analytics platforms for real-time insights	– Dynamic impact tracking – Integration into planning and performance management – Enabling portfolio-level interrogation by business users

Table 14: Focus areas for scenario production enhancement

Enhancement Area	Description	Strategic Impact
Scenario Structuring & Taxonomy	Revisiting frameworks built post-2008 to improve granularity, modularity, and sector specificity, including climate and environmental risk	– Captures more realistic assumptions – Reflects interconnected and ripple effects – Enables modular reuse across portfolio
Faster Production Cycles	Streamlining workflows through automation, process re-architecture, and GenAI-assisted variable expansion	– Reduces timelines from weeks to days – Enables agile, responsive execution – Allows "lightweight stress testing" with speed over precision
Modular Architecture & Automation	Building component-based architectures for dynamic scenario configuration and recombination	– Greater scalability and reuse – Lower cost of scenario deployment – Accelerated updates and iteration
Analytics & Self-Service Tooling	Platforms for intelligent querying, automated comparison, and what-if testing of scenario results	– Empowers frontline/portfolio teams to run simplified scenarios – Enhances transparency and engagement – Supports risk-informed business planning

Expanding early warning systems while preparing to harness insights from a growing reservoir of external data

Backward-looking metrics and forward-looking processes that run on a periodic basis are no longer sufficient to help identify, prioritise, and respond to emerging threats—often before those threats manifest as losses or compliance breaches. Harnessing growing volumes of internal and external data, institutions are strengthening investment in early warning systems operating in near-time, scanning large data volumes for weak signals, anomalies, or deteriorating trends across a broad set of risk domains.

This is leading to a growing sophistication of early warning systems, with pattern detection expanding to predictive analytics and digital risk assistants. Unlike stress testing and scenario analysis—which focus on hypothetical future states—early warning systems (EWS) are about real-time signal detection and prioritisation. Their primary value lies in filtering noise, enabling faster intervention, and directing human attention to the most relevant issues. EWS tools are being deployed across a growing range of applications: regulatory and legal change monitoring, deteriorating credit quality, third-party risk indicators, and external/internal threat intelligence within GRC and operational resilience domains.

Participants described the development of these systems as a layered continuum of increasing sophistication:

- At the foundational level, simple filtering tools help streamline credit and compliance monitoring. This supports productivity by helping filter out the most relevant information from increasing data volumes. At the same time, high-volume activities such as monitoring data flows and transactions require pattern analytics for effective risk management.
- Further up the maturity curve, predictive analytics join internal and external signals to forecast potential risk events. AI is increasingly being deployed to join up different data sets to identify patterns and look for indications of potential incidents before they take place. This is not limited to non-financial risks, as complex areas such as cash and collateral movements have seen success in explainability and predictability.

- At the most advanced stage, institutions are experimenting with digital risk assistants—autonomous agents that help orchestrate assurance work and risk decisions. These tools not only support risk managers in prioritising their day-to-day focus but also offer the potential to reshape how assurance and control activities are deployed in dynamic environments.

Table 15: Maturity Spectrum of Early Warning Capabilities

Capability Layer	Description	Example Applications
Filtering Engines	Automated systems that filter and prioritise relevant risk signals from internal and external data sources	– Client and segment-level credit monitoring – Transaction analytics for fraud and AML – Initial triage of legal and regulatory updates
Predictive Analytics	Analytics that combine structured and unstructured indicators to forecast deterioration and potential compliance/control breaches	– Proactive issue detection in resilience, operational risk, or conduct – Cash and collateral explainability and predictability
Digital Risk Assistants	Intelligent agents that synthesise data inputs and recommend prioritised actions or decision paths for risk managers	– Trigger-based assurance models – Real-time risk dashboards – Shaping day-to-day risk activities based on environmental signals

Streaming real-time data: Towards the analytical toolkit of the future

As institutions expand analytical capabilities, they are increasingly turning to alternative and near-time data sources to gain more precise, real-world insights. From satellite imagery and drones to blockchain-based supply chain data and sensor-fed ESG inputs, the opportunity to capture conditions on the ground—often in real time—is expanding rapidly. These new data streams are powerful, but they also introduce novel risks, and infrastructure challenges that legacy systems were not built to handle.

To unlock value from these sources, firms must develop the ability to ingest, interpret, and act on unstructured data, while ensuring traceability, trust, and interoperability. A major constraint today is the lack of harmonised industry protocols for how data—especially external or third party—should be captured, tagged, and exchanged. For example, efforts to track emissions at source using distributed sensor technology require industry protocols governing taxonomies and standards for measurement, capture and sharing. This is key to establish trust, auditability and make the data useful in production.

Equally, new forms of risk and control mechanisms are required to manage the unique vulnerabilities of alternative data—such as data poisoning, manipulation, or fragmentation. Institutions must avoid introducing risk by feeding unverified data into core systems. This is leading to the emergence of new validation frameworks, tamper-proof capture mechanisms (e.g. using distributed ledger tech), and AI-powered anomaly detection layers. These guardrails will be essential if alternative data is to be used in production-grade risk and assurance environments at scale.

Table 16: Enabling the Use of Alternative Data in Risk Management

Capability / Focus Area	Description	Implications for Risk and Controls
Alternative Data Integration	Incorporation of external, unstructured, and sensor-based data (e.g., video, audio, ESG, satellite) to complement traditional risk inputs	– Enhanced visibility of ground conditions – Improved early warning on ESG, resilience, and supply chain exposures
Harmonised Protocols	Industry-wide standards for how alternative data is captured, structured, and transmitted	– Enablement of auditability and comparability – Reduced data integration burden – Facilitation of regulatory alignment and industry benchmarking
Distributed Ledger Use	Use of blockchain and DLT for tracking provenance and creating tamper-proof, time-stamped records	– Strengthening of trust in external signals – Assurance of data integrity and traceability across ESG and supply chain use cases
Control Mechanisms for New Data	New risk controls that address manipulation, spoofing, and data quality degradation in real-time or external data flows	– Avoidance of corrupted data entering core systems – Support for governance of AI inputs – Critical for high-trust automation and assurance processes

Evolving resilience – Confronting strategic dependencies and thinking the unthinkable

Resilience remains firmly at the top of the industry agenda considering events since our last study. What once might have been viewed as a compliance domain is now at the centre of strategic conversation. The reasons are clear: geopolitical tensions escalating into open conflict, widespread cyber incidents, and an increasing reliance on a concentrated set of third-party providers have all exposed the fragility of complex systems. What's different now is not just the intensity of these risks—but the realisation that many are outside any one institution's control.

The unspoken assumption that foundational services—cloud infrastructure, core banking platforms, third party connectivity—will always be available is also beginning to be questioned. Leaders are now asking difficult, previously unthinkable questions. What happens if access to major cloud platforms is restricted due to geopolitical sanctions? Could we function if a major cloud provider were to suffer a systemic failure? What would an escalation of current conflicts mean for our operating model? How would a coordinated attack on undersea telecommunications cables play out?

These scenarios may seem remote, but they no longer feel implausible. They force institutions to engage with the edges of their risk appetite—and to confront the reality that not everything can be controlled or insured against.

Recent outages and access threats have demonstrated that regulation alone is not a safeguard. There is recognition of the limits to what institutions (and industry) can do – and a call to be transparent about this. This coincides with a call for dialogue with politicians and regulators to address burning questions on the regulatory perimeter, as well as medium-term strategies to reduce potentially toxic combinations of geopolitical friction and industry dependencies.

Table 17: Resilience Response Grid – What Firms Are Doing

Strategic Focus Area	What Firms Are Doing	Purpose / Impact
Strategic Questioning	Asking more fundamental questions: What do we rely on? What if it fails? How fast can we adapt?	Encourages more forward-looking, design-driven thinking in how organisations plan for the unknown
Integration with Risk Frameworks	Aligning resilience with taxonomies, operational risk, and recovery/resolution planning	Embeds resilience into core business and risk processes, creating a more coherent and actionable foundation
Scenario Planning & Playbooks	Conducting structured exercises on cloud failure, data centre loss, political risk and conflict scenarios	Builds preparedness beyond plausible assumptions; improves responsiveness in uncertain environments
Digital Simulation & Digital Twins	Starting to model value chains digitally to run simulations and scenario tests	Enables advanced stress testing and proactive identification of hidden vulnerabilities, following practices in aerospace and energy sectors
Protecting the Core: "Minimum Viable Institution"	Defining essential services (e.g. payment capabilities, access to balances); designing fallback protocols	Support preservation of that basic functionality even during severe outages or geopolitical disruptions
Industry Collaboration	Joining industry-level response simulations; engaging providers to pressure-test risk assumptions	Encourages shared standards, greater transparency, and more realistic assessments of collective exposure
Rewiring External Dependencies	Advocating for regional technology providers ("regional champions"); supporting diversification away from concentrated global tech ecosystems	Reduces strategic dependence on a small set of vendors; enables long-term resilience at national or regional level
Cyber & Supply Chain Resilience	Investing in visibility and response capabilities across third- and fourth-party ecosystems; hardening digital architecture	Expands the perimeter of resilience beyond organisational boundaries, addressing risks across the full delivery chain

05 From One-Way Regulatory Oversight to Two-Way Dialogue - A need to revisit the relationship between industry and regulators

Over the last fifteen years, the financial services industry has operated under an expanding wave of regulatory oversight, marked by growing volume, complexity, and granularity of requirements. While the foundational principles of regulation remain widely endorsed, there is growing consensus that frameworks and supervisory models need strategic reflection. The industry has evolved, but regulatory design and engagement have not always kept pace.

Four themes stand out in how institutions are now rethinking regulation:

- **Framework fitness and oversight models** — questioning whether regimes designed for legacy banking structures remain fit for purpose today.
- **Blurring of sector boundaries** — as third parties, platforms, and big tech move from service providers to systemic actors at the heart of financial stability.

- **Evolving regulatory engagement models** — with calls to rebalance one-way, prescriptive oversight towards more iterative, co-created approaches.
- **Regulatory culture and mindset** — ensuring supervisors have the expertise, agility, and pragmatism to keep pace with industry transformation.

The following sections explore each theme in turn.

Framework fitness and oversight models

Financial institutions are now deeply intertwined with third-party providers, who play core roles in infrastructure, platforms, and decisioning tools that directly shape risk profiles. Regulations like the EU AI Act and DORA acknowledge this shift, but oversight models have yet to adapt operationally.

At the same time, the traditional one-way model of regulation—rules handed down with little feedback—is under strain. ESG rules showed the risk: burdensome taxonomies and stress-testing requirements diverted resources, with limited value in hindsight. This has sparked calls for more participative approaches, where early-stage industry feedback is built in and unintended consequences surfaced sooner.

Finally, many feel regulators themselves must evolve faster. Industry wants more domain expertise, pragmatic judgment, and leadership rotation to bring fresh thinking. In a period of structural and technological change, such qualities are critical to keeping oversight relevant, proportionate, and responsive.

Table 18: Industry perspectives on regulatory frameworks and engagement models

Theme	Description	Emerging Tension	Strategic Signal
Evolving Industry Structure	Integration of third parties into core banking activities	Regulatory models lag behind operational reality	Growing demand for adaptive oversight mechanisms
Framework Fitness	Reassessment of regulatory frameworks after 15 years of expansion	Regulations designed for a legacy banking model	Need to re-anchor regulatory design in current industry dynamics
Dialogue and Feedback	Demand for two-way interaction and feedback loops	Insufficient consideration of industry issues and trade-offs	Interest in co-regulatory models and independent feedback bodies
Regulatory Culture & Mindset	Calls for pragmatic, business-sensitive oversight	Perception of academic/theoretical focus in regulators	Need for greater mobility and infusion of private sector expertise

Blurring of boundaries between the financial services and technology sectors – A call to rethink the supervisory perimeter and points of entry

The original financial regulation architecture was built for a world where high infrastructure costs created strong barriers to entry. This foundation has eroded. Digital technologies, cloud-native systems, and modular service models have lowered those barriers, enabling a wave of agile new entrants—from fintechs to tech giants—into areas traditionally dominated by banks.

Figure 6: Preparing for the competitors of tomorrow – A shift away from traditional banks[6]

	Average ranking	Number 1 choice
Digital Banking Startups	1.8	7
Large Tech companies	2.3	4
Large Internationally Active Banks	2.4	6
Crypto Ecosystems	3.8	0

In parallel, regulatory changes have rendered certain banking activities less profitable. As a result, many banks have exited individual markets, leaving space for less intensively or unregulated players. Compounding this is the growing integration of third-party tech providers—delivering infrastructure, software, and AI—who now sit at the heart of modern banking. Their reliability and conduct have become direct factors in financial stability.

In our 2022 Global Risk Study, concerns centred on banks' dependency on big tech as critical service providers, particularly limitations around control and assurance. That concern remains, yet technology companies are now regarded as both critical suppliers and direct competitors. They are no longer just supporting the financial system—they are shaping it.

This shift has major implications for regulatory design. Oversight remains fragmented across and within jurisdictions, raising fundamental questions: Should oversight lie with financial regulators, technology supervisors, or a blended model? How should supervisors coordinate across different jurisdictions? These questions challenge outdated perimeter assumptions and highlight the need for clearer "point-of-entry" models. While initial initiatives such as the critical third party regime in the UK are underway, there is a view on the need to do more.

Still, a key uncertainty remains: Can global standards emerge in a period marked by geopolitical division and AI competition?

6 The chart is an aggregation of ranking from 1 to 6 provided by participants. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the main emerging competitor

Table 19: A transforming industry pushing the boundaries of current regulatory frameworks

Theme	Description	Emerging Tension	Implications for regulatory engagement
Lowered Barriers to Entry	Digitalisation erodes traditional banking exclusivity	Increased competition from unregulated/non-bank players	Traditional banking perimeter is no longer clear-cut
Regulatory Displacement	Regulation reshapes profitability and activity mix	Banks withdraw, non-regulated actors step in	Supervision may not align with systemic risk
Critical Technology Providers	Infrastructure, software, and AI now integral to banking	Control and assurance mechanisms lag	Need to redefine regulatory responsibilities
Big Tech as Competitor	Shift from service provider to direct competitor	Regulatory scope and regime boundaries unclear	Hybrid or sector-blending regulation models emerging
Capability Gaps in Oversight	Regulatory bodies struggle to match tech sophistication	Lack of standardised supervisory models	Investment in supervisory talent and digital tools required
Toward Global Standards	Consideration of an international regulatory framework	Political divergence impedes coordination	Likely emergence of bottom-up standards in areas like data integrity
Catalyst for Change	First systemic failure in AI as potential turning point	Status quo inertia	Crisis may trigger institutional realignment

Evolving the regulatory engagement model - Strengthening two-way dialogue and co-creation mechanisms

There is strong agreement that the principles underlying regulatory frameworks—financial stability, consumer protection, and resilience—remain valid. At the same time, there is rising support for uplifting engagement mechanisms in an industry undergoing accelerating change. Regulators face the hard job of overseeing an increasingly complex sector amid geopolitical divergence, but industry participants argue that current models of interaction are no longer sufficient.

Three dynamics are driving the call for a more collaborative, outcome-oriented regulatory model. First, the evolving banking model: digitisation and platformisation have increased the velocity and complexity of banking, yet regulatory expectations often lag or lack flexibility, creating challenges for innovation and resource allocation. Second, the shift from financial to non-financial risk: as institutions mature in managing traditional financial exposures, supervisory pressure has shifted to cyber, operational resilience, and third-party risk—areas that are dynamic, systemic, and require years of capability-building. Third, the rise of systemic themes such as ESG and AI: both sit at the crossroads of politics, ethics, and risk, demanding phased, long-term approaches, while compliance is often required before standards and infrastructure are ready.

Across geographies, perspectives differ, but two priorities for reform are clear. Institutions want better strategic alignment and prioritisation, with more open dialogue on trade-offs, sequencing, and consistent interpretations across supervisory colleges. They also call for greater agility in new and rapidly evolving domains, particularly ESG and AI, where joint development and iterative implementation of standards would help avoid costly, premature fixes.

While no easy or short-term solutions exist, a range of mechanisms have been proposed: structured review cycles with industry and legislative feedback; CRO-led roundtables with regulators; and independent third-party bodies to balance ambition with practicality. These proposals do not call for deregulation, but rather for recalibrating engagement to match a fast-evolving landscape—keeping regulation robust while enabling innovation and resilience.

Table 20: Drivers of change of regulatory engagement model

Theme	Description	Emerging Tension	Strategic Signal
Regulatory Engagement Fatigue	Institutions are overwhelmed by the pace and complexity of requirements	Compliance overload impedes strategic transformation	Need for collaborative, fit-for-purpose oversight
Business Model Change	Digitisation and platformisation increase velocity and complexity	Frameworks lag or lack flexibility, stifling innovation	Push for phased, outcome-based compliance pathways
NFR Ascendancy	NFRs (cyber, resilience, third-party) now rival financial risks	Capability development lags regulatory expectation	Iterative, capability-focused supervision needed
Thematic Complexity (ESG & AI)	ESG and AI reshape the financial landscape; they require phased, multidisciplinary responses	Compliance pressure often precedes maturity of frameworks	Joint development and co-created standards
Inconsistencies in Interpretation	Divergence across jurisdictions and supervisory colleges	Conflicting requirements for global firms	Standardisation of supervisory practice and definitions
Proposals for Model Reform	Formal review cycles with feedback, CRO-led roundtables, independent third-party arbitration bodies	Current oversight models are rigid and one-way	Experimental models of co-design and regulatory feedback

Culture and mindset at regulators – Enabling pragmatic oversight in a digital age

As regulatory frameworks adapt to increasingly complex and interconnected risks, there is broad consensus across the financial services industry that supervisory culture, mindset, and skillset must evolve as well. While regulatory principles may be shifting in intent, their design and enforcement often remain anchored in legacy assumptions—particularly around expertise and the operational posture of supervisors.

A recurring theme across geographies is the desire for more senior-level mobility within regulators, bringing in fresh thinking and aligning practices more closely with industry evolution.

Institutions further highlight the urgent need for greater expertise in non-financial risks, as banks pivot toward resilience, cyber, model risk, and reputational exposures. Closely related is the push for a more participative regulatory role in innovation and capability development—moving beyond passive oversight to active involvement in sandboxes, co-innovation labs, and simulation environments.

Finally digitisation is rising on the agenda. While initiatives like Banks Integrated Regulatory Dictionary “BIRD” provide blueprints for harmonised reporting, fragmented taxonomies and inconsistent definitions remain a major bottleneck. Regulators are being called on to embrace their own transformation journeys, investing in training, digital enablers, and international collaboration to avoid being outpaced by the institutions they supervise.

Table 21: Evolving regulatory capabilities in lockstep with a transforming financial services industry

Theme	Description	Emerging Tension	Strategic Signal
Leadership Mobility	Desire for senior-level mobility within regulators to inject fresh thinking	Static leadership slows institutional renewal	Rotational roles to align culture with industry change
Recruitment Imbalance	Call to complement legalistic/ academic profiles with practical business experience	Gap between rule-setters and implementers	Recruitment of cross-sector talent to bridge policy–practice divide
NFR Skill Gaps	Acute need for supervisory expertise in resilience, cyber, model risk, and reputational exposures	Misalignment as banks pivot resources toward NFRs	Cross-functional regulatory teams essential
Proactive Engagement	Shift from post-hoc intervention to co-development of controls and guardrails (eg, sandboxes, labs, simulations)	Passive oversight fails in fast-moving domains	Hands-on engagement accelerates capability building and trust
Supervision by Design	Move toward digital-first oversight using real-time data ingestion and machine-readable regulation	Fragmented taxonomies and inconsistent definitions across jurisdictions	Shared standards and ontologies critical for scalable digital supervision
Institutional Transformation	Opportunities to reform recruitment, considering public-private rotation, invest in training, and join international standard-setting	Risk of regulators being outpaced by industry innovation	Adaptive capacity, mindset, and digital enablers determine future effectiveness

06 Adapting to the ESG divide - Responding to a complex theme in a fragmenting world

ESG remains one of the most complex and nuanced challenges facing the banking industry. It offers strategic opportunities, but also a growing set of risks that are difficult to capture in a systematic and harmonised way. Capabilities remain nascent, data and methodologies underdeveloped, and lengthy transition pathways expose banks to uncertainty often beyond their control. Political outcomes, for example, can reshape medium-term ESG strategies overnight.

Despite polarisation, most institutions expect material changes to business and operating models within the next decade. Progress has been made embedding ESG into frameworks and processes, but inconsistencies in taxonomies and definitions persist. Firms are also calling for a political and regulatory "reset" before additional nature-related requirements add further complexity.

Four topics dominate how banks are adapting to this ESG divide:

- **Strategic tensions** — navigating political and regulatory divergence while balancing transition and physical risks.
- **Embedding ESG in frameworks** — integrating ESG consistently into risk management, with a focus on harmonised taxonomies, definitions, and standards.
- **ESG risk management and analytics** — improving data, stress testing, planning, and decision-making to move ESG from principle to practice.
- **Stakeholder expectations and opportunities** — managing demands from investors, staff, and society, while pursuing opportunities in transition finance, trading, and risk transfer.

Strategic tensions - Navigating the political and regulatory divergence

The current geopolitical environment is a wake-up call for institutions to face reality. The change in US administration shifted the course for the next four years, and potentially beyond, highlighting the fragility of assumptions underpinning global transition planning. Outlooks built on pathways like SSP2 underpinning projections used for international climate goals no longer hold, and institutions must now consider the implications of a world transitioning into geopolitical blocs.

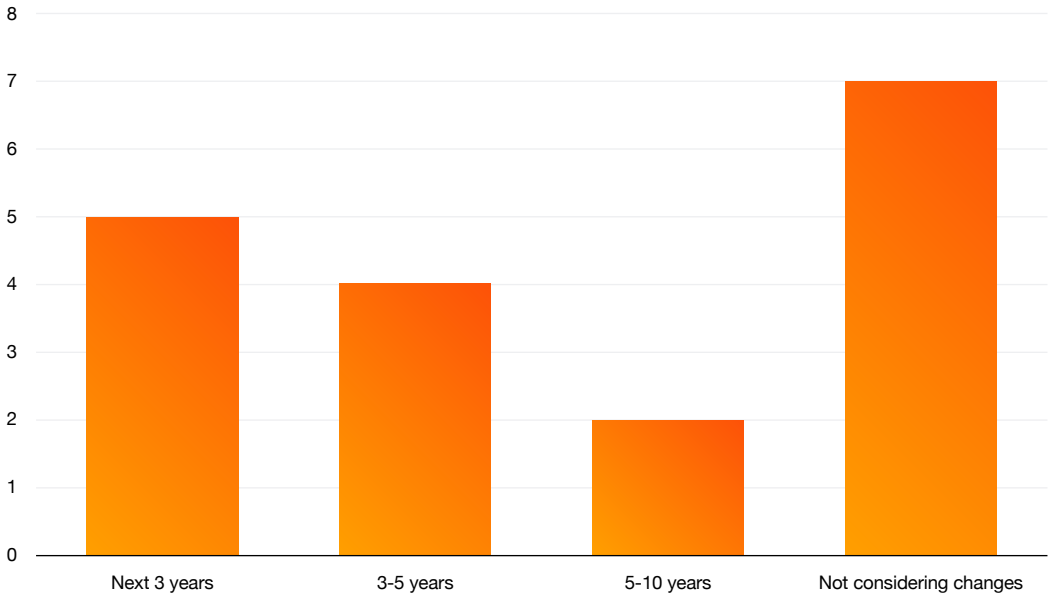
Figure 7: Top climate and environmental risks to the organisation[7]

	Average ranking	Number 1 choice
Impact of Physical Events	2.8	4
Policy Divergence	3.3	6
Sharp Transition	3.3	3
Legal Risks	3.7	1
Stranded Assets	3.8	2
Loss of Insurability	4.1	2

- The increasing impact of **physical events** is seen as the top risk across the industry. More frequent and intense weather phenomena are exposing society's lack of preparedness for both extreme events and chronic conditions such as prolonged heatwaves and droughts.
- In the short to medium term, **policy divergence** between the US and EU is a major challenge. The boundaries between politics and regulation are increasingly blurred, leaving global institutions unable to reconcile conflicting expectations. This creates reputational risk and operational complexity, compounded by stakeholders' differing views on issues like diversity, equity, and inclusion (DEI).
- Institutions also highlighted concerns around **clients' ability to deliver transition plans,** which exposes banks directly and indirectly, as well as **exposure to sharp discontinuities** driven by elections or political shifts. These risks underscore the need for dialogue and pragmatism between regulators, lawmakers, and the industry.

7 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

Figure 8: Expectation of making changes to business and operating models[8]



Despite turbulence, most participants remain committed to their ESG strategies. While some high-profile names have reduced or delayed commitments, the majority expect business and operating model changes within the next decade. Increasingly, the **opportunity side of ESG** is being emphasised—transition partnerships, trading markets, and risk transfer innovation are seen as key levers for long-term value creation.

Table 22: Strategic tensions in ESG

Theme	What Firms Are Doing	Strategic Significance
Policy & Political Divergence	Managing conflicting ESG expectations across US and EU operations	Heightened reputational, legal, and operational complexity
Activist & Legal Risk	Navigating cross-jurisdictional pressure from stakeholders and litigation threats	Risk of lawsuits, reputational exposure, and brand damage
Transition Risk Delivery	Assessing clients' ability to deliver transition plans	Direct and indirect impacts on banks' own net-zero strategies
Physical Risk Escalation	Facing increased intensity and frequency of extreme weather events	Dual pressure on resilience and long-term strategy
Transition vs. Physical Risk Balancing	Running scenarios that weigh sudden policy reversals against long-term climate impacts	Shapes capital allocation, appetite, and strategy decisions
Discontinuity Planning	Preparing for election-driven reversals in ESG commitments	Review and revise medium-term assumptions and strategy
Persistent Strategic Commitment	Most participants holding course despite political shifts	Reinforces long-term vision with pragmatic adjustments
Opportunity Emphasis	Building partnerships with governments and development banks; exploring emissions and hydrogen trading	Seen as critical to raising awareness, building maturity, and financing transition infrastructure
New Risk Transfer Mechanisms	Developing alternatives to traditional insurance protocols to cover structural shifts in climate risk	Expands resilience and creates new product opportunities
Societal Underpreparedness	Recognising systemic lack of readiness for climate and nature shocks	Emphasises need for enhanced scenario planning and risk appetite frameworks

8 Count based on the number of institutions indicating a specific time frame for making changes to business and operating models

Progress in embedding ESG in risk frameworks, with growing calls for consistent protocols and taxonomies across industries and jurisdictions

Despite continued progress since the last study, ESG remains one of the most complex and structurally unresolved areas within the risk landscape. It does not map neatly onto traditional risk categories. Instead, it cuts across them, amplifying existing exposures or creating new impact channels.

Frameworks such as the TCFD (Task Force on Climate-related Financial Disclosures) have been valuable in providing a common reference, but they have not covered all dimensions of ESG. In some cases, they have also been translated too literally into risk taxonomies, leading to inconsistent application within firms and across the industry. The result is fragmented integration and a lack of clarity about what ESG truly encompasses.

Figure 9: Differences in Banks approaches to embed ESG risks in the risk taxonomy[9]

	As part of other risks	Standalone principal risk	Not covered
Climate Risk	12	6	1
Environmental Risk	14	4	1
Nature Risk	10	2	6
Social Risk	14	3	2

9 Table based on the number of institutions indicating a specific approach to embedding ESG risks into the enterprise risk taxonomy

Climate risks are better analysed by most banks as compared to Nature and Social risk, but impact channels remain vague and relationships to other risks are poorly articulated. Nature risk is an emerging concern, with TNFD (The Taskforce on Nature-related Financial Disclosures) guidance expected to feed into regulation. However, standards and data remain fragmented, creating fears of bureaucratic compliance costs without meaningful insight. Meanwhile, social and governance dimensions continue to provoke debate — some stakeholders argue they are too broad to fit under a common umbrella and should perhaps be treated separately.

The absence of consistent **taxonomies, definitions, and methodologies** mirrors the challenges faced in non-financial risk. Institutions stress the need for convergence, common standards, and pooled data sources to advance ESG as a discipline. Drawing on lessons from climate regulation, there are calls for stronger co-creation between regulators and industry, particularly as nature risk becomes a focus.

Table 23: Challenges and responses in embedding ESG

Theme	What Firms Are Doing	Implications for Risk Management
Fragmented Integration	ESG is inconsistently embedded across teams, with climate furthest along; "S" and "G" remain unclear. ESG often framed as amplifying existing risks	Leads to incoherent control frameworks, blurred accountability, and difficulty linking ESG to enterprise risk
Standards, Data & Collaboration	Industry is advocating for common taxonomies and exploring pooled data solutions, but faces reluctance to share costs or sensitive data	Without harmonised definitions or usable shared data, ESG tooling remains patchy and hard to scale
Nature Risk & New Regulation	Firms are preparing for TNFD-aligned nature risk regulation, amid uncertainty in definitions and metrics	Risk of costly compliance with little operational insight if regulations are rolled out without early industry input
Governance & Cultural Shift	ESG is seen as a cross-cutting capability like NFR; firms are calling for co-designed standards and investing in staff enablement	Long-term success depends on industry-regulator alignment and cultural ownership of ESG within the business

ESG risk management and analytics – Data, planning and the path to maturity

The past five years have seen meaningful steps in embedding ESG into operational decision-making and enterprise processes. Many firms now integrate ESG into risk identification, horizon scanning, and corporate planning. Yet this integration remains uneven, limited by gaps in data quality, inconsistent methodologies, and planning horizons that do not align with the long-term nature of ESG risks.

Figure 10: Priorities in embedding ESG risks in the organisation[10]

	Average ranking	Number 1 choice
Efficient and accurate disclosures	2.6	5
Identifying and developing accurate data sources	3.2	4
Developing ESG understanding in staff	3.8	1
Integration of ESG with horizon scanning	4.1	2
Developing business-friendly tools supporting decision-making	4.2	2
Integration of ESG with corporate planning	4.4	2
Building risk quantification and pricing capabilities	4.6	2

Data availability and quality remain core challenges, undermining the ability to measure and quantify ESG risks consistently. Most firms continue to rely on qualitative tools such as scoring frameworks and heatmapping, which help raise awareness but are insufficient for robust quantification. At the same time, disclosures and reporting continue to dominate the agenda, reflecting their strategic importance to positioning and reputational management.

Stress testing and scenario analysis are improving but still tend to follow regulator-driven, long-term approaches, with few institutions running short-dated shock scenarios. This limits their usefulness for corporate planning and ICAAP (Internal Capital Adequacy Assessment Process). There is a growing recognition of the need to sharpen stress testing capabilities — for example, modelling the effects of sudden emissions pricing shocks or reinsurer failures triggered by natural disasters.

Figure 11: Number of climate risk scenarios run annually[11]

	0	1-5	5-10	>10
Instantaneous	11	4	0	0
Short term (up to 5 years)	4	9	2	1
Medium Term (5-10 years)	7	6	2	0
Long term (beyond 10 years)	3	10	2	1

10 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

11 Table based on the number of institutions indicating running a specific number of scenarios across the specified time frames

ESG is increasingly embedded in lending decisions across the industry, using a combination of tooling with an emphasis on qualitative and scoring frameworks. The lower degree of ESG consideration in markets businesses highlights the inherent complexity, as well as the remaining need to overcome a degree of first line scepticism of Risk tooling and methodologies.

Figure 12: Practices to integrate ESG into commercial decisions[12]

	Retail	Wholesale	Trading and execution
Quantitative assessment (e.g., PD / LGD / VaR)[13]	6	6	0
Qualitative assessment (e.g., slotting, heatmapping)	15	16	4
Transition scoring / ESG ratings (counterparty, sector, region)	9	12	4
Stress testing / scenario analysis	13	16	6

Institutions are also working to **embed ESG more directly in lending and business decisions,** though adoption varies. Lending portfolios increasingly use ESG scoring and transition ratings, while markets and trading businesses show more scepticism, reflecting the complexity and uncertainty of risk tooling in these areas.

Encouragingly, new capabilities are emerging. These include:

- **Geographic heat maps** linking assets to transition and physical risks.
- **Frameworks** aligning top-level transition views with sector/regional slotting methodologies.
- **Granular trading system data** that allows deeper analytics and collateral transparency.

Overall, progress is clear, but a step-change in **data, methodology, and scenario practices** is needed to make ESG integration consistent, tangible, and decision-relevant.

12 The table is based on the number of responses by participants; missing numbers to total respondents are where a certain practice is not in place

13 PD = Probability of Default; LGD = Loss Given Default; VaR = Value at Risk)

Table 24: Investing in enhanced capabilities to manage climate and environmental risks

Theme	What Firms Are Doing	Implications for Risk Management
Horizon Scanning & Planning	Establishing "house views" of transition pathways by geography and sector	Provides consistent planning anchor and informs appetite
Linkage to Corporate Planning	Strengthening ties between ESG planning, risk appetite, and operational decision-making	Aligns strategy with sector/geography risk outlooks
Stress Testing – Long-term Bias	Running regulator-driven, long-term scenarios	Misaligned with ICAAP and near-term capital adequacy decisions
Stress Testing – Shock Scenarios	Beginning to run short-dated shocks (eg, emissions price spikes, reinsurer failure from natural disaster)	More relevant to corporate planning and ICAAP
Scenario Complexity	Classifying risks by order of magnitude and focusing on tipping points	Improves prioritisation and strategic readiness
Data & Methodology Gaps	Data quality, capture protocols, and taxonomy inconsistencies limit progress	Reliance on qualitative tools; undermines comparability and robustness
Sectoral & Regional Analytics	Building in-house analytics for sector/regional ESG dynamics	Enables more granular and forward-looking risk assessments
Enhanced Decision Tools	Mapping exposures using geographic heat maps; linking transition views to slotting frameworks	Creates intuitive and actionable insight across the business
Granular Trading System Data	Expanding look-through into collateral and ABS portfolios	Provides visibility into complex exposures and supports targeted analytics
Staff Awareness & Education	Raising staff understanding through clearer definitions, training, and intuitive tooling	Overcomes scepticism, builds accountability, and embeds ESG into first-line processes
Reliance on Qualitative Tools	Using qualitative scoring, heatmapping, and transition ratings in lending	Builds awareness but highlights urgency for stronger quantitative methods
Market Business Adoption	Lower uptake in trading/markets businesses due to complexity	Risk of uneven integration and limited enterprise coherence

Stakeholder expectations and opportunities

Despite political turbulence and divergence across jurisdictions, most firms expect business and operating model changes within the next decade. High-profile names in banking and other industries have adjusted or deemphasised ESG commitments, but the majority remain focused on executing strategies set in recent years.

The **opportunity side of climate and environmental risks** is gaining emphasis across the industry. Transition financing, carbon and hydrogen trading markets, and innovative risk transfer mechanisms are increasingly seen as critical to building organisational maturity and embedding ESG awareness. Banks also recognise the importance of working with a broader set of stakeholders — not only governments and regulators, but also investors, employees, and society at large. These groups exert strong expectations on financial services to deliver progress on ESG, even in the face of political fragmentation.

For many, **pragmatism in the short-to-medium term must** be balanced with **ambition in the long term**. Institutions are acknowledging that the world is entering a "bumpy" phase of transition, where consensus is hard to achieve. Yet there is no expectation of a fundamental reversal.

Table 25: ESG strategy – Key win themes

Theme	What Firms Are Doing	Strategic Significance
Enabling the Transition	Partnering with governments and corporates on financing and trading (e.g. emissions, hydrogen); exploring risk transfer mechanisms beyond insurance	Drives infrastructure change, strengthens transition pathways, and supports resilience where traditional insurance falls short
Sustaining Commitment Amid Uncertainty	Holding firm on ESG strategies despite political headwinds; recognising transition will be non-linear and consensus will vary	Signals long-term credibility, strategic consistency, and adaptability in volatile environments
Broadening the Stakeholder Lens	Engaging investors, staff, and civil society—not just regulators; embedding ESG into culture and employer brand	Builds trust, attracts talent, and supports licence to operate in contested ESG debates
Using ESG as a Strategic Narrative	Enhancing disclosures and ESG reporting to align with investor demands and corporate positioning	Shapes investor sentiment, reputation, and capital flows in a polarised world

07 The Strive for Risk Efficiency

Efficiency has been a top priority for Risk functions for more than a decade. What began as a narrow focus on cost has matured into a willingness to tackle the "hard" challenges of **data, legacy systems, and process redesign.** Our 2025 study highlights a further shift: efficiency is increasingly framed in terms of **productivity, business experience, and organisational agility.**

Flat or declining budgets remain the norm. Although cost pressures appear less acute than in 2022, the lower absolute levels hide the need to free up capacity for reinvestment. At the same time, digital banks and technology companies are reshaping the competitive environment, intensifying the push for automation and cost efficiency.

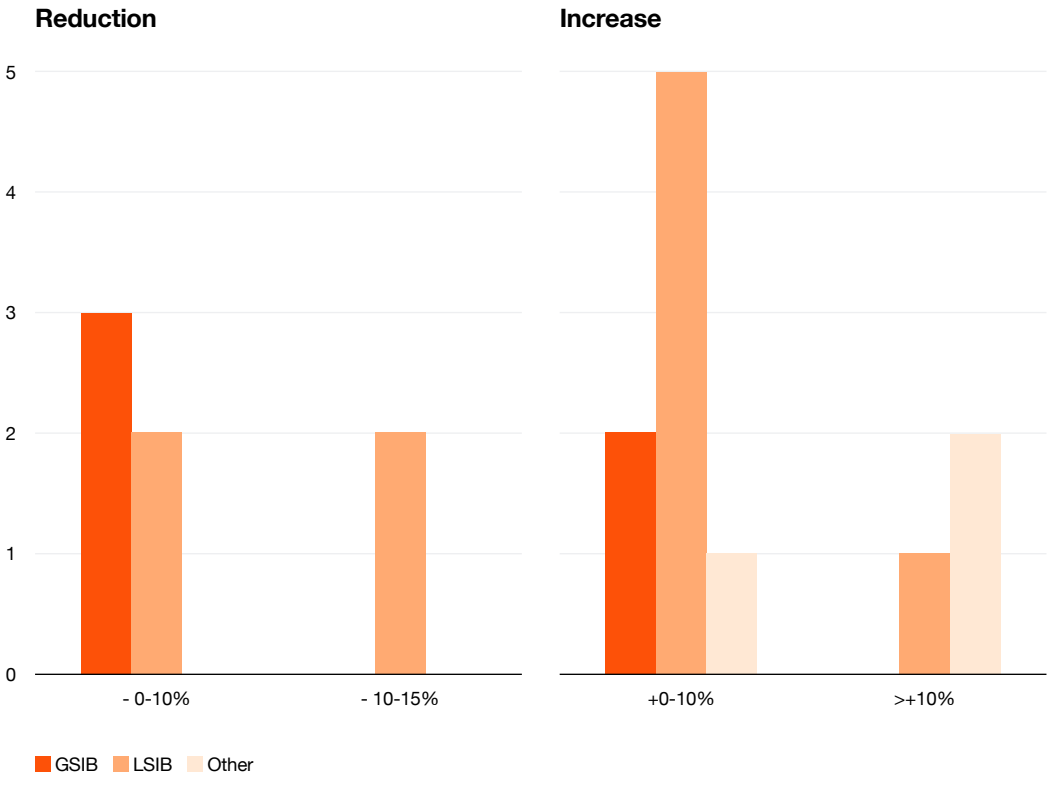
This chapter explores four themes that define the industry's current approach to risk efficiency:

- **Creating capacity beyond costs** — broadening efficiency programs to include reinvestment capacity, speed, and decision-making.
- **Unlocking efficiencies in costly processes** — especially credit, modelling, and quantitative analytics.
- **Rethinking assurance and reporting** — targeting automation, standardisation, and control utilities across lines of defence.
- **Making productivity tangible** — digitising processes to create transparency, metrics, and continuous optimisation.

Creating capacity in an environment of intensifying competition, with efficiency programs broadening the scope beyond costs

Cost targets in 2025 are less ambitious than in 2022, but pressure remains on large institutions to release capacity. Smaller, nimble institutions are scaling up investment, often after painful lessons from control failures.

Figure 13: Cost targets over the next 3 years[14]



14 Number of institutions per cost reduction / increase bucket

The scope of efficiency programs has expanded. Outcomes now explicitly target **faster decision-making and speed to market**, reflecting competition from digital banks and tech firms. Data and technology are widely viewed as future differentiators, but progress has been uneven: large-scale transformation programs are expensive and slow, with diverging ambitions for simplification and data harmonisation.

Process excellence and change management skills are emerging as critical enablers, yet under-invested in across Risk functions.

Table 26: Key industry actions in shaping efficiency initiatives

Theme	What Firms Are Doing	Strategic Significance
Cost Targets	Setting smaller targets than 2022 but still pressured to create reinvestment capacity	Sustains transformation agendas
Scaling by Smaller Firms	Expanding Risk investment after incidents	Builds resilience and trust
Expanded Efficiency Scope	Linking efficiency to speed, agility, and decision-making	Moves beyond cost-only mindset
Competitive Pressures	Responding to digital banks and tech firms as competitors	Forces acceleration of transformation
Data & Tech Transformation	Large-scale architecture and data model simplification	Seen as decisive long-term advantage
Process Excellence & Change Management	Growing focus on cross-functional process discipline	Critical to execution, but under-invested

Unlocking efficiencies in costly processes

Efficiency approaches have matured: they are now **data-led, rigorous, and end-to-end.** Programs target both demand-side (business and infra) and supply-side (Risk) levers. Costliest processes vary by institution, but **credit and modelling** dominate given their heavy headcount.

Figure 14: Most costly processes for Risk oversight and challenge[15]

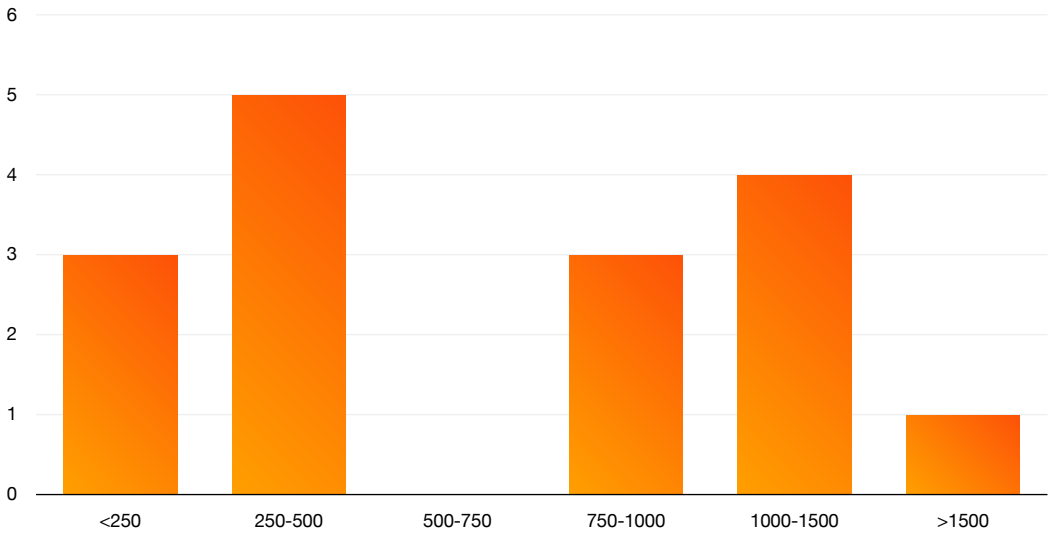
	Average ranking	Number 1 choice
Model development and maintenance	2.9	4
Origination (Retail)	3.2	4
Market risk oversight and analytics	3.3	2
Origination (Wholesale)	3.3	4
RCSA	3.8	2
Control Assurance	4.1	1
Corporate planning	6.0	0

Credit risk – simplification, automation and first-line empowerment

- **Retail and SME origination:** automation is advancing, supported by better data and new technologies. Oversight is shifting from transaction-level to portfolio-level, enabling more holistic control across credit, fraud, conduct, and operational risks.
- **Wholesale:** levers include questioning client/product footprint, aligning first- and second-line "production chains," and using GenAI to transform burdensome tasks such as credit analysis and memos. Delegated authority is being emphasised across the credit lifecycle.

Model development and maintenance – a complex and burdensome estate, with GenAI removing previous barriers to automation

Figure 15: Number of models by institution[16]



15 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

16 Number of institutions indicating a model inventory count falling into the specified buckets

- Model estates remain extensive and complex, often numbering hundreds to thousands. Rationalisation efforts have had mixed success.
- GenAI is driving structural change, automating documentation, testing, and development. As one participant noted: “GenAI is commoditising expertise.”
- Early second-line engagement models show opportunities to reduce the burden of model lifecycle processes.
- In the short term, capacity must be freed to implement GenAI safely. Long term, Risk teams may shrink, with data and analytics taking the lead.

Table 27: Costly processes and automation

Area	What Firms Are Doing	Strategic Significance
Retail Credit	Automating origination, QA, and controls	Improves efficiency and oversight
SME Lending	Leveraging new data to automate decisioning	Raises scalability and consistency
Wholesale Credit	Rationalising portfolios, aligning lines of defence, using GenAI for analysis and memos	Frees capacity and reduces drag
Delegated Authority	Ist line self-certification combined with portfolio level 2nd line oversight for low-materiality counterparties	Speeds up decisions while retaining control
Model Rationalisation	Simplifying and consolidating model estates	Reduces complexity and costs
GenAI in Modelling	Automating documentation, testing, and coding	Fundamental shift: “commoditising expertise”
Interaction Model Reform	Early second-line involvement in model lifecycle	Improves outcomes without losing independence
Future Workforce Shift	Anticipating smaller traditional Risk teams, more data/analytics-driven	Long-term redesign of budgets and roles

Rethinking assurance processes and reporting "production" – towards structural automation of "low-value" tasks

Assurance remains burdensome, with many firms maintaining large assurance and testing structures in the first (and sometimes also second) lines of defence.

Institutions are now rethinking models, focusing on:

1. **Centralisation of controls and utilities** across lines of defence, enabling fungible teams and consistent taxonomies.
2. **Automation of GRC processes** — traditional automation plus GenAI to reimagine workflows.

Figure 16: Current and target automation of selected assurance processes[17]

	Achieved				Targeting			
	0-25%	25-50%	50-75%	75-100%	0-25%	25-50%	50-75%	75-100%
Risk and Control Self-Assessment	6	7	2	0	0	1	11	2
Control Oversight / Testing	7	6	2	0	0	3	7	4
Operational Resilience Monitoring	9	3	2	0	0	3	7	3

Poor-quality control inventories remain a barrier. Some firms have achieved 80% reductions through inventory "cleaning" and minimum standards.

Reporting and MI (Management Information) is another high-effort area. Production is largely federated and manual, but institutions see potential in centralised utilities. GenAI is already being piloted for first-draft commentary on reports. Views diverge: some have centralised reporting into Finance; others remain sceptical, citing expertise needs.

Table 28: Efficiency initiatives in reporting and assurance

Theme	What Firms Are Doing	Strategic Significance
Control Utilities	Cross-LoD utilities to standardise assurance	Economies of scale; convergence of practices
Automation Ambitions	Applying automation and GenAI in GRC	Reduces low-value tasks, frees capacity
Control Inventories	Cleaning, standardising, and reducing duplicates	Improves quality and enables automation
Regional Differences	Large EU CCO structures vs US remediation-heavy testing teams	Reflects regulatory drivers
Centralised MI Utilities	Exploring utilities for MI/report production	Frees capacity; enables dashboards, self-service
GenAI in Reporting	Drafting first-pass commentary	Accelerates reporting; augments staff effort
Organisational Debate	Diverging views on centralising reporting in Finance vs. retaining in Risk	Highlights trade-off between expertise and scale

17 Table shows the % automation ranges of selected processes that a count of institutions have achieved and targeted. Differences in the count between achieved and targeted may arise given missing responses

Making productivity tangible – creating visibility by digitising the organisation

For years, firms have attempted to measure productivity through **timesheets** or **output metrics**. These methods provided only partial visibility and faced challenges in complex Risk activities.

A new approach is emerging, leveraging process digitisation to create visibility into **production systems:**

- Mapping effort across value streams (e.g., mortgage origination, portfolio management).
- Capturing activity granularity with workflow tools.
- Designing metrics that account for throughput, seasonality, and comparative performance.

While still early, large institutions expect to build these capabilities over the next five years, enabling continuous optimisation and sharper cost management.

Table 29: Growing sophistication in productivity management

Theme	What Firms Are Doing	Implications
Timesheet Analysis	Capturing periodic effort allocation at process level	Provides only headline views
Metric-Based Measurement	Defining outputs for standardised teams (eg, call centres)	Limited applicability to heterogeneous Risk tasks
Digitisation & Workflow	Digitising processes to capture throughput and effort granularity	Enables transparency within production systems
Value Stream Focus	Capturing productivity at value-stream level (eg, origination)	Aligns with NFR/operational resilience systems
Metric Design	Incorporating seasonality, throughput, and comparability	Turns operational data into management insights
Future Ambition	Establishing productivity monitoring in large firms within five years	Continuous optimisation; more rigorous cost discipline

08 The Risk Workforce in a Transitioning Industry

Our 2022 industry study highlighted the beginnings of a generational transition. Experienced incumbents, shaped by multiple crisis periods, were handing over to a new generation who had not lived through similar shocks, but brought different expectations and digitally native skillsets. Competition for talent from outside financial services was also beginning to reshape recruitment and retention priorities.

In 2025, the Risk workforce remains top of mind. Across the industry, three themes stand out:

- **Leadership and the CRO profile** — evolving beyond traditional financial risk backgrounds, preparing for hybrid workforces, and providing confidence through uncertainty.
- **Workforce transformation and talent management** — succession planning, rotations, and new recruitment channels to build rounded leaders and retain talent.
- **Skills of the future** — combining digital fluency and specialist NFR expertise with increasingly important soft skills and holistic thinking.

Leading through uncertainty and structural change

The CRO role is more prominent in 2025 than in our 2022 study. CROs are expected to provide vision and lead staff through transition, delivering risk management in very different ways. Confidence, trust, and reassurance are essential in a context of cost reduction, industry transformation, and technological disruption.

Against this backdrop, interviewees stressed that the leadership role of the CRO is now **much more prominen**t than in 2022. CROs must not only instil confidence and trust but also **allay fear** in this environment of transformation and cost reduction.

With increasing expectations for CROs to be involved in commercial aspects as part of senior management, the need to influence a broad stakeholder set, and the ongoing shift from financial to non-financial risks, thinking around the future CRO profile is evolving. While there is no consensus, several perspectives emerged.

Table 30: Perspectives on the future CRO profile

Theme	Summary
Background	A financial risk background remains important to most institutions, but a subset is increasingly open to CROs from non-financial risk, enabled by strong leadership layers in credit and market risk
Organisational tenure	Several firms strongly favour internal tenure. One firm stated they would not consider outside hires at C-suite level, citing the importance of understanding the organisation's DNA
Diverse experiences	Business leadership roles are regarded as favourable, balancing oversight with commercial enablement. Exposure to finance, process, infrastructure, and third-party management is valuable in the pivot to NFR
Leadership expectations	CROs must champion new ways of working, instil confidence, **allay fear,** and manage accelerating change over the coming years

Leadership is also being re-imagined in the context of GenAI adoption. Over the next decade, financial services expect a shift toward **hybrid workforce models,** where humans oversee and collaborate with digital agents, supported by increasingly capable risk assistants. Leadership models must adapt to manage these human–machine teams, potentially through new collaboration structures including augmented-reality environments.

Figure 17: Perspectives on key enablers for workforce collaboration[18]

	Already in place	Next 5 years
Cross lines of defence team structures	5	8
Collaboration tooling	11	6
Augmented reality		9
AI Agents	4	13
Integration with third parties	7	6

18 Count based on number of institutions indicating a specific choice

Figure 18: Key measures industry is taking to change mindsets and culture[19]

	Average ranking	Number 1 choice
Thinking outside organistational silos	3.0	5
Embracing Artificial intelligence	3.6	4
Driving and enabling innovation	3.9	2
Managing change and continuous improvement	3.9	3
Thinking outside organisational boundaries	5.0	1
Balancing risk and reward	5.1	2
Increasingly digital teams/ways of working	5.2	1
Cost Conscious behaviour	6.1	0

This transition requires taking the workforce on a multi-year journey, with strong emphasis on changing culture and mindset.

Table 31: Success criteria for culture and mindset shifts

Theme	Summary
Tone from the top	Executives must embrace new ways of working, breaking silo mentalities through visible collaboration. Oversight should be pragmatic and materiality-focused. Importantly, CROs must not just promote but also actively use GenAI
Role of mid-level management	Mid-level managers are critical in diffusing tone from the top but are often comfortable with BAU. Levers include active objective setting for transformation with mid-level management, while aligning incentives to reward stepping up and taking risks
Tangible measures	Cross-functional team structures, innovation time, and workshops promoting tech adoption. Targeted deployment of agents in specific processes is testing hybrid ways of working and informing oversight/control evolution
Behavioural segmentation	Several firms classify staff cohorts by ease of technology uptake. Cost-consciousness, though not always explicit, is deeply embedded in the culture of several highly digital and innovative banks

19 The chart is an aggregation of ranking from 1 to 6 provided by 20 participants to a survey questionnaire. The average is a simple linear average, while the number 1 choice column provides a count of how many participants identified an option as the key challenge. Any deviations to 20 are non-responses or multiple mentions as a number 1 choice

Growing sophistication of workforce management practices

In our 2022 study, a workforce transition was expected — from an analogue generation to a digitally native one with different expectations. There was **initial concern about a "war for talent",** as financial services competed more directly with technology firms.

By 2025, this "war for talent" is less pronounced, but the need to enhance workforce management practices is clearer. The strongest themes are **recruitment channels, succession planning,** and **talent development.**

Recruitment channels

Recruitment channels are one of the clearest signals of this shift. Firms are reassessing traditional pipelines from financial services and giving greater weight to internal rotations, technology/AI expertise, and process excellence skills from other industries. This mix reflects the repositioning of Risk and the strategies for adopting emerging technologies.

Table 32: Industry perspectives on the evolution of Risk recruitment channels

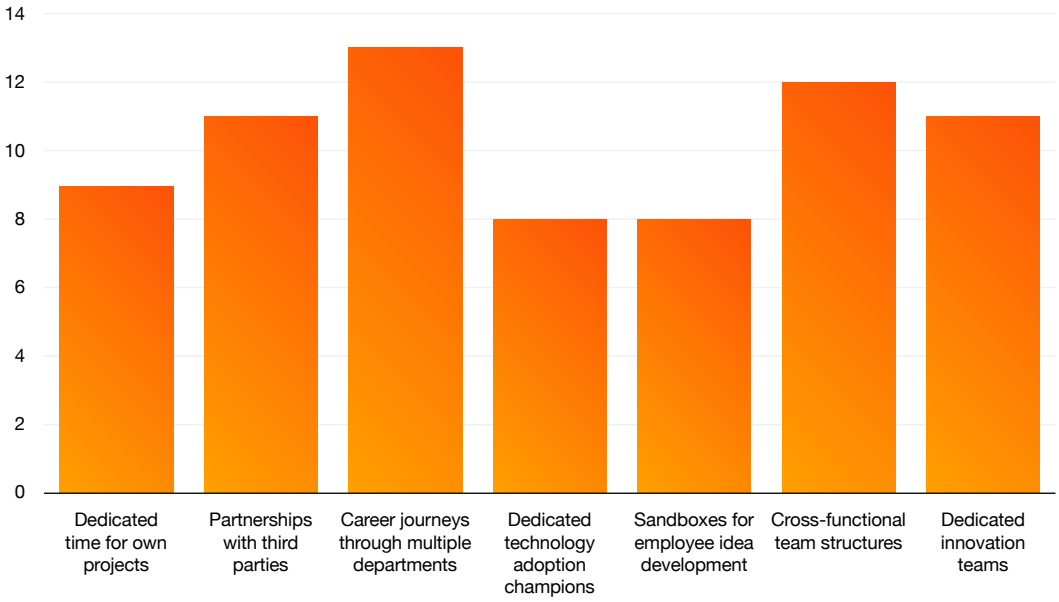
Channel	Observations
Financial services	Still the predominant source of talent, especially for leadership
Internal recruitment	Emphasis is on building holistic profiles and strengthening business experience in Risk. Reflected in succession planning and talent management measures
Tech / AI firms	For some G-SIBs this is the top choice, aligned with AI "democratisation" strategies
Consulting firms	Valued for process/change management and taxonomies. Often chosen as a secondary channel
Other industries	Sectors like aviation, pharmaceuticals, and defence score highly on process excellence. Some firms hire six-sigma black belts from manufacturing to drive efficiency and digitisation. However, these hires often face resistance internally, requiring more awareness of their value as ways of working and risk profiles change

Succession planning and career journeys

Succession planning is gaining prominence, covering not only CROs but also Heads of Risk stripes.

- **Tenure vs. fresh perspectives:** some firms prioritise internal tenure; others want external hires for fresh thinking.
- **Organisation size:** leaders from large banks may struggle in smaller firms, which require more hands-on, "duct tape" leadership styles.
- **Career breadth:** Emphasis on CRO candidates with CEO, CFO, or business head experience given breadth of exposure to finance, operations, and risk.
- **Lateral moves:** mid-management rotations are often resisted but can be encouraged through clear expectations and incentives.
- **Management of personality mix:** some institutions explicitly embed personality requirements into succession planning.

Figure 19: Measures in place to build an innovative workforce[20]



Not every firm has successfully implemented rotations — some cite limited appetite or feasibility even within Risk teams (e.g. between credit/market and NFR). However, participants strongly value the benefits of rotation, with one long-tenured leader highlighting how a career move reinvigorated his effectiveness.

Applied approaches to building workforce expertise

- **Workshops, hackathons, and demonstrations:** encourage GenAI uptake (e.g., interrogating data sets, showing how to apply GenAI to specific tasks).
- **Self-service analytics:** dashboards with drill-downs, providing staff with powerful tooling.
- **Project roles:** opportunities for staff to take on change assignments, building rounded profiles and continuous improvement mindsets.

The impact of AI on entry-level jobs is debated. Some firms see no major concern; others expect large-scale automation to force graduate and training programmes to reset. Entry-level tasks traditionally build practical banking experience gradually — automation may undermine this, requiring new approaches to provide strong foundations for new entrants.

20 The x-axis shows number of institutions having taken individual measures

The Risk workforce of the future — holistic, digital, and critical thinkers

Industry thinking has matured since 2022. Most institutions can now articulate a target profile: a digitally fluent, holistic, and adaptive Risk workforce.

Figure 20: Perspectives on current and target skillsets[21]

	Current				Target			
	<10%	10-25%	25-50%	50+%	<10%	10-25%	25-50%	50+%
Data and Analytics	5	1	7	1	2	2	5	5
Audit	9	2	0	2	6	5	0	2
Quantitative Modelling	6	6	0	1	3	8	2	0
Regulatory and Policy	4	4	2	3	3	4	3	3
Front Office / Product Expertise	2	3	4	4	1	3	3	6
Regional / Sector / Segment Strategy	7	2	4	0	6	2	5	0
Technology and Software	8	3	2	0	5	4	3	1
PMO / Change / Business Consulting	8	1	3	1	6	4	1	2
Cyber and Information security	10	1	1	1	5	5	2	1

Conversations consistently highlighted six transformation priorities that together define how the Risk function is being reshaped — from leadership and rotations, to technology adoption, culture, and future skills.

Table 33: Workforce transformation priorities

Theme / Priority	What Firms Are Doing	Strategic Significance
CRO & Leadership Evolution	Expanding CRO profiles beyond financial risk, emphasising digital fluency and strategic influence	Positions Risk as a strategic partner in transformation
Rotation & Career Journeys	Building T-shaped profiles through cross-functional rotations and diverse career paths	Develops holistic risk leaders and improves retention
GenAI Adoption & Hybrid Workforce	Deploying digital risk assistants, agents, and automation in first/second line	Transforms workforce models, redefining human–machine collaboration
Cultural & Mindset Shift	Embedding tone from the top, incentivising innovation, and breaking silos	Facilitates adaptation of risk culture to speed and complexity of change
Talent Management & Succession	Active CRO and stripe-head succession planning; recruiting from tech and other industries	Builds resilience in leadership pipeline, enhances expertise in digital and NFR
Skills for the Future	Investing in soft skills (storytelling, collaboration, problem solving) alongside technical literacy	Creates adaptive, future-ready workforce

21 The table shows the count of institutions having indicated a specific % range for individual skills

Structural shifts

- Affinity with technology and handling large datasets are baseline skills, with GenAI fluency becoming a prerequisite across roles.
- GenAI fluency will become a prerequisite across roles.
- Cybersecurity and information security will grow in importance at across all layers of the organisation.
- Broader, **T-shaped profiles** will replace narrow functional SMEs.
- Non-financial risk literacy remains low in many institutions, but automation is freeing up capacity to reinvest in specialist skills.

Table 34: Continued emphasis on soft skills, amplified by GenAI

Level	Skills & Priorities
Leadership	Holistic thinking, cross-silo collaboration, innovation and technology adoption
Mid-level management	Transformation and digitisation skills; operational excellence remains a gap
Operational staff	Agility, engineering mindset, problem-solving, critical thinking, and storytelling to cut through information overload

Soft skills are **not straightforward to develop.** Some firms actively manage personality types across teams. One CRO noted their teams receive training in "how to ask the right questions."

A debate has emerged over **AI commoditising technical expertise.** Some argue that coding and quantitative analysis will decline in importance, as AI makes these skills widely available. Others disagree, but consensus exists that soft skills are critical differentiators for the workforce of the future.

Consensus: the risk manager of the future will be both **digitally adept** and **culturally agile,** bridging human and machine capabilities.

Conclusion

Risk functions are entering a decisive phase of transformation. The forces reshaping them are structural, not temporary: the acceleration of technology, the broadening of risk beyond financial into non-financial and resilience, the growing interdependence with third parties, and the need for new skills and leadership models. Institutions can no longer rely on static frameworks or incremental change.

The path forward requires Risk to operate with greater **clarity, speed, and intelligence** — embedding digital capabilities, rethinking operating models, and fostering cultures where accountability and collaboration are instinctive. At the same time, leadership must cultivate the judgement, adaptability, and soft skills that technology cannot replicate.

What is emerging is a Risk function that is both **guardian and enabler:** safeguarding trust and resilience while creating the conditions for innovation and growth. Its success will depend on the courage to simplify, the discipline to modernise, and the willingness to engage openly with regulators, ecosystems, and society. The challenge is significant, but so too is the opportunity: to position Risk as a catalyst for sustainable progress in an uncertain world.

Authors

Johannes Goldner
PwC UK
Johannes.n.goldner@pwc.com

Ajay Raina
PwC UK
Ajay.raina@pwc.com

Contacts

Europe

Rami Feghali
France
Rami.feghali@pwc.com

Dominik Kaefer
Germany
Dominik.kaefer@pwc.com

Dirk Stemmer
Germany
Dirk.stemmer@pwc.com

Symon Dawson
UK
Symon.k.dawson@pwc.com

Peter el-Khoury
Uk
Peter.elkhoury@pwc.com

Pietro Penza
Italy
Pietro.penza@pwc.com

Matteo d'Alessio
Italy
Matteo.dalessio@pwc.com

Casper Ruizendaal
Netherlands
Casper.ruizendaal@pwc.com

Anthony Kruizinga
Netherlands
Anthony.Kruizinga@pwc.com

Gregory Joos
Belgium
Gregory.joos@pwc.com

Northern America

Matt Devine
Canada
Matt.devine@pwc.com

Alejandro Johnston
US
Alejandro.johnston@pwc.com

Dietmar Serbee
US
Dietmar.d.serbee@pwc.com

Alex Pflepsen
US
Alex.m.pflepsen@pwc.com

Pranjal Shukla
US
Pranjal.m.shukla@pwc.com

APAC

Julia Leong
Singapore
Julia.sw.leong@pwc.com

Jun Muranaga
Japan
Jun.muranaga@pwc.com

Marna Slabbert
Australia
Marna.slabbert@au.pwc.com

Tony Richardson
Australia
Tony.richardson@au.pwc.com

David Bellingham
Australia
David.bellingham@au.pwc.com

Africa

Jacques Muller
South Africa
Jacques.muller@pwc.com

Kumar Tulsi
South Africa
Kumar.tulsi@pwc.com

Global Banking Risk study